NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

**CRITICAL FAILURE MODE ANALYSIS
OF THE
PETITE AMATEUR NAVY SATELLITE
(PANSAT)**

by

David W. Alldridge

September 1995

Principal Advisor: Barry Leonard

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September, 1995	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Critical Failure Mode Analysis Of The Petite Amateur Navy Satellite (PANSAT)	5. FUNDING NUMBERS
6. AUTHOR(S) Alldridge, David W.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT

System reliability analysis is an essential element is the design process. A reliability study should proceed from system inception through final deployment. As the PANSAT project approaches the final design stage and begins initial flight production, the absence of any significant reliability analysis becomes increasingly troubling. This thesis initiates the program's reliability analysis obligation by investigating spacecraft failure modes. Typically referenced as critical failure modes, these events will cause complete and permanent system failure. A reliability analysis tool, called Fault Tree Analysis (FTA), is used to conduct a systematic review of current hardware design architecture to expose potential critical failure points or weak links.

The analytical result is a Boolean logic tree that describes critical failure events and all the potential causes. This causal output relationship describes each component failure (i.e., single point failures), or component failure combinations (i.e., multi-point failures), which could cause the undesirable failure event, or Top Event. The fault tree will provide design engineers and management personnel with an effective tool and reference point from which to implement design modifications to circumvent potential problems.

14. SUBJECT TERMS Petite Amateur Navy Satellite, PANSAT, Reliability, Failure Analysis, Hazard Analysis, Critical Failure Analysis, Critical Failure Mode Analysis, Fault Tree Analysis	15. NUMBER OF PAGES 174
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

CRITICAL FAILURE MODE ANALYSIS
OF THE
PETITE AMATEUR NAVY SATELLITE (PANSAT)

David W. Alldridge
Lieutenant, United States Navy
B.S., Oregon State University, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(SPACE SYSTEMS OPERATIONS)

from the

NAVAL POSTGRADUATE SCHOOL
September, 1995

Author: ____________________________
David W. Alldridge

Approved by: Barry Leon
Barry Leonard, Principal Advisor

W. M. Woods
Walter M. Woods, Second Reader

____
Rudolph Panholzer, Chairman
Space Systems Academic Group Operations

ABSTRACT

System reliability analysis is an essential element is the design process. A reliability study should proceed from system inception through final deployment. As the PANSAT project approaches the final design stage and begins initial flight production, the absence of any significant reliability analysis becomes increasingly troubling. This thesis initiates the program's reliability analysis obligation by investigating spacecraft failure modes. Typically referenced as critical failure modes, these events will cause complete and permanent system failure. A reliability analysis tool, called Fault Tree Analysis (FTA), is used to conduct a systematic review of current hardware design architecture to expose potential critical failure points or weak links.

The analytical result is a Boolean logic tree that describes critical failure events and all the potential causes. This causal output relationship describes each component failure (i.e., single point failures), or component failure combinations (i.e., multi-point failures), which could cause the undesirable failure event, or Top Event. The fault tree will provide design engineers and management personnel with an effective tool and reference point from which to implement design modifications to circumvent potential problems.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

I. INTRODUCTION

A. PANSAT OVERVIEW

The Petite Amateur Navy Satellite (PANSAT) is a small satellite being designed, fabricated, and eventually operated by faculty and students at the Naval Postgraduate School (NPS). Primarily a project of the Space Systems Academic Group (SSAG), it combines the efforts and expertise of staff and students of various departments. These include the Departments of Aeronautical and Astronautical Engineering, Electrical and Computer Engineering, and Computer Science. The spacecraft will provide amateur radio enthusiasts a new space communication medium utilizing spread spectrum modulation for radio packet switching. It also provides a platform for evaluating the use of spread spectrum in reducing frequency band congestion.

The design, development, and deployment of the satellite is integrated in a coordinated manner by the SSAG engineering staff and master's candidate students at NPS. The student contributions are primarily through thesis, class, or individual projects as well as directed study courses. The faculty provides the necessary expertise and direction to assist in project and thesis advisement and consultation.

1. Purpose

The primary purpose of the PANSAT project is to provide a practical hands-on experience for NPS students in the Space Systems Operations and the Space Systems Engineering curriculums. Military communication applications employ spread spectrum techniques primarily to achieve anti-jam and security objectives. PANSAT provides the officer student with practical hands-on experience for future applications of this technology.

a. Engineering

The engineering experiences provided by PANSAT allow students of various core engineering factions the opportunity to apply basic principles, coupled with creative thought processes, to a wide variety of engineering problems inherent to the design and fabrication of a spacecraft. The student is able to experience the spacecraft development process from conceptual design through fabrication, testing, launch integration and deployment stages.

b. Operation

Students of the Space Systems Operation curriculum benefit from the opportunity to experience a wide variety of aspects of space system acquisition and operation that would not normally be made available in an academic environment. The PANSAT program provides a creative medium to explore new and exciting concepts from mission planning, requirements definition, and design reviews through spacecraft launch, initialization, and mission operations. This provides a valuable background to the student in future assignments as program sponsors, project managers, or operational supervisors.

2. Mission Overview

The mission of the PANSAT spacecraft will be to carry a communications payload that exploits the amateur radio community's 70 centimeter band. The implementation of a communication link which spreads a differentially coded binary phase shift keyed (BPSK) signal utilizing the direct sequence spread spectrum (DSSS) technique, is an element of the PANSAT design which makes it unique from other spacecraft that employ radio packet switching communications.

a. Concept of Operations

Developed as a small, about 150 pounds, spread spectrum communications satellite for officer students at NPS as an educational project, PANSAT will be launched into Low Earth Orbit (LEO) from the Space Shuttle via the Hitchhiker program. The capability to launch the spacecraft from a refurbished Minuteman missile is under investigation as an alternate launch platform.

The exact orbital parameters of the spacecraft are not yet known, it is expected however to operate in a circular orbit at an orbital altitude of approximately 200 nautical miles, with an inclination of between 28.5 and 51.6 degrees. Amateur radio ground stations will be able to access PANSAT to utilize its capabilities as a orbiting e-mail server providing store and forward packet file transfer (Fig. 1) between terrestrial users. Packet switching, utilizing the amateur radio community's packet switching protocol (AX.25) will be used as the networking protocol between the ground station and the spacecraft.

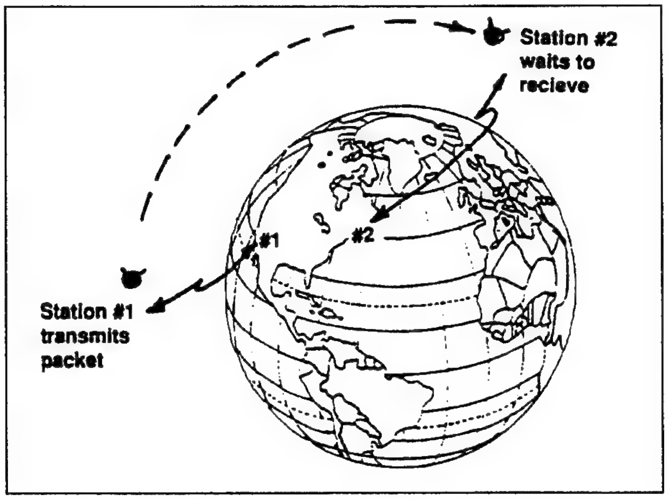


Figure 1. Store and Forward Concept [Ref. 1]

The PANSAT design objective was to minimize cost and complexity, this in turn fostered creativity and resourcefulness. The absence of Guidance Navigation and Control (attitude control), Thermal Control (active), and Propulsion subsystems created unique issues to be addressed by the design engineers. With orbital attitude that has been commonly referred to as "tumbling", the spacecraft employs distinctive antenna design characteristics to help ensure the communications payload will be consistently in contact with visible ground stations.

B. THESIS OBJECTIVE

In the most general terms, the reliability of a system can be described as the probability a system will remain operational or maintain it's ability to complete its design mission objective for a given period of time under given environmental conditions. The applications of the reliability analysis field and methods used to evaluate them are extensive. This thesis will explore the application of one such method, called Fault Tree Analysis (FTA), to critically evaluate the PANSAT design.

1. Purpose

Reliability analysis of a system can be accomplished utilizing various analysis methods. A particular analytical method may be more applicable to a particular design state than another during the project's life-cycle. To date no detailed reliability analysis has been conducted, prefacing an unquestionable need to perform a subjective study. The identification of potential failure modes prior to the critical design review, and commencement of flight hardware production, is essential to ensure fulfillment of the mission life requirement.

2. Concurrent Engineering Concept

The idea of concurrent engineering, or the practice of incorporating various life-cycle values into the early stages of design, is one that has gained an increasingly popular following, particularly in the climate of shrinking fiscal budgets. The process of designing for reliability is an element of the process that is receiving a great deal of attention. Particularly in systems, like satellites, where system repair is next to impossible once the system is placed into operation, the concern for a reliable system by all levels of management is at the forefront of the design process (Fig. 2).

Principally an organizational and managerial challenge, concurrent engineering concepts are particularly important in the early stages of program development. Traditionally, reliability budgeting begins in the concept phase and reliability verification continues throughout the project development cycle.

A cursory study of the project design may lead a program manager or design engineer to believe the system is very robust due to the built in redundancy of the design architecture. A detailed study may reveal inherent weak points that could aggravate the true system reliability.

3. Scope of Thesis

This thesis will analyze the critical hardware failure modes of the PANSAT hardware architecture by utilizing an analysis tool called Fault Tree Analysis (FTA). Critical failure is summarized as those failures which lead to an inoperable and unrecoverable failure of essential mission components that leave the system inoperable. This can occur at any time within the systems lifetime.

Although not immediately apparent, a reliability study for a project which is as relatively small and seemingly simple as the PANSAT design, can quickly become complex and increasingly time consuming.

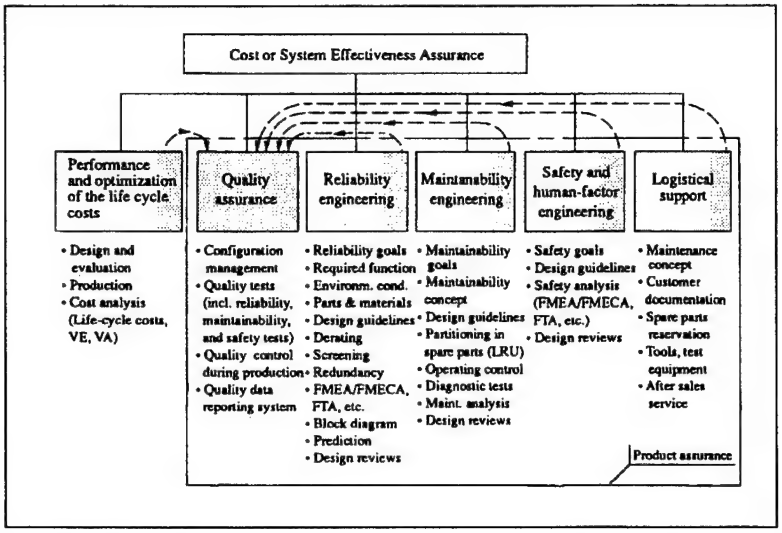


Figure 2. Cost or System Effectiveness Assurance Structure [Ref. 2]

a. Problem Statement

A detailed reliability study of the PANSAT project has not been conducted to this point, so this thesis will be a first cut analysis of the current design status. The majority of the critical failure analysis will focus on an analysis of the Electrical Power Subsystem (EPS), with a minor look at the Digital Control Subsystem (DCS) and the Communications Subsystem (COMM) payload. The incomplete design status, particularly low level design considerations, of various subsystems (i.e., particular functional and component design as well as component identification) precludes a detailed quantitative reliability analysis. The fault tree will be constructed incorporating a qualitative analysis of the hardware design, with the capability to conduct subsequent quantitative analysis as required. The goal of a qualitative review will be to help identify weak areas of the design, particularly single point failures, in which a design work around could easily be incorporated.

b. Research Questions

There are two primary questions this thesis will address in order to help minimize the potential for a critical failure.

(1) What are the critical failure modes of the PANSAT hardware architecture?

(2) How can critical failures be minimized through hardware and software design modifications?

C. THESIS STRUCTURE

The remaining portions of this thesis will adhere to the following composition.

1. Chapter II: PANSAT BACKGROUND

This chapter will provide the reader with a synopsis of the hardware and software architecture of the PANSAT program. This will provide a working understanding of the system design in it's present state. A review of the subsystem design, particularly the EPS, will be beneficial in understanding the system operation and the magnitude of the analysis required. A short description of the program timeline is included to provide the reader an understanding of the program life-cycle and the unique nature of a program whose primary development is supported by student involvement that is continuously changing.

2. Chapter III: Reliability

This chapter is devoted to the development of reliability issues involved in conducting a design analysis. A theoretical basis of the FTA methodology is discussed including its application to real world issues. There are numerous software packages available to assist a reliability engineer in the analysis of a system. A software package, called FaultrEASE, employing a FTA program, was used for the fault tree construction and analysis and is discussed for completeness.

3. Chapter IV: PANSAT Fault Tree Analysis

A detailed exploration of the fault tree constructed for the PANSAT project will be investigated in this chapter to answer the research questions. Detailed analysis of the fault tree is provided to explore issues of potential problems.

4. Chapter V: Summary

This chapter will summarize the reliability issues uncovered during the analysis and the recommendations made for design modification. Follow on reliability analysis is suggested to assist in management decisions and further student research.

5. Appendix A: Electrical Power Subsystem (EPS) Fault Tree Analysis

This appendix contains EPS block diagrams and schematics to assist the reader in understanding the system configuration. A fault tree of the EPS is included with analysis information summarized in tables describing the failure end events and failure event combinations which could cause a critical failure of the EPS.

6. Appendix B: Communication Fault Tree Fault Tree Analysis

This appendix contains a block diagram of the radio frequency (RF) subsystem to assist the reader in understanding the system configuration. A fault tree of the RF subsystem is included with analysis information summarized in tables describing the failure end events and failure event combinations which could cause a critical failure of the RF subsystem.

7. Appendix C: Digital Control Subsystem Fault Tree Analysis

This appendix contains a block diagram of the digital control subsystem (DCS) to assist the reader in understanding the system configuration. A fault tree of the DCS is included with analysis information summarized in tables describing the failure end events and failure event combinations which could cause a critical failure of the DCS.

8. Appendix D: PANSAT FAULT TREE

This appendix contains the fault tree constructed using the FaultrEASE software package. All the analysis results listed in the previous appendices were derived from this fault tree.

II. PANSAT BACKGROUND

A. DEVELOPMENT

The PANSAT program was conceived in 1989 as an interdisciplinary educational opportunity for NPS Space Systems Operations and Space Systems Engineering postgraduate students. Future duty assignments of students in these cirriculum will be in support of space system acquisition, design, and operation.

The spacecraft consist of four major subsystems: Communications (COMM), Electrical Power Subsystem (EPS), Digital Control Subsystem (DCS), and the Structure subsystem. Contrary to other spacecraft designs, the PANSAT project does not contain two major subsystems found on most spacecraft. The Guidance, Navigation, and Control (GNC) and the Propulsion subsystems have been eliminated from the design to reduce complexity and cost. Additionally there is no active thermal control subsystem.

B. SYSTEM ARCHITECTURE

The hardware architecture is the principle focus for the reliability analysis, with a brief description of the envisioned software architecture mentioned for completeness.

1. Hardware Architecture

a. Structure

The PANSAT structure provides the housing and support mechanisms for the other spacecraft (S/C) systems. Constituting a 26 sided polyhedron in which 18 of the sides are square and the remaining eight sides are triangular, the aluminum frame provides structural support for the internal electronic components as well as the externally mounted 17 solar panels which are attached to the square sides (Fig. 3). The one remaining square side is reserved for the launch vehicle interface (LVI). A design proposal is being studied for the utility of mounting a smaller solar panel within the void region of the LVI. If the additional solar panel concept is accepted, this gallium arsenide panel will provide additional power to the power system that is operating on a very tight power budget.

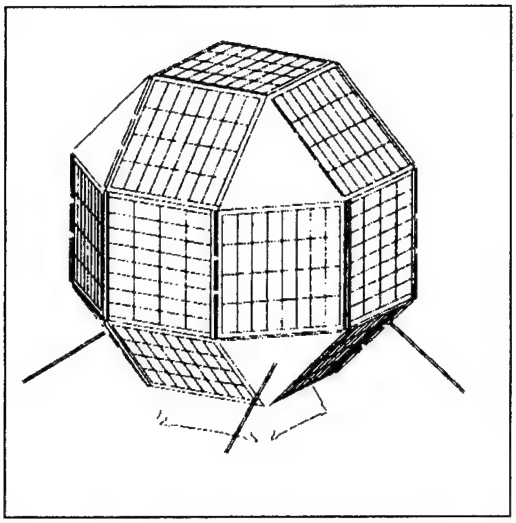


Figure 3. PANSAT External Structure [Ref. 1]

The approximately 19 inch diameter polyhedron was chosen to allow the mounting of the solar panels on the external skin of the S/C, allowing solar energy conversion in any orientation of the spacecraft and to minimize the range of values of solar flux area. The upper triangular sections of the external structure support the four dipole antennas, that are mounted in a tangential turnstile configuration.

Internal equipment mounting support (Fig. 4) is provided by two equipment plates (upper and lower) with each major subsystem component housed within an equipment box.

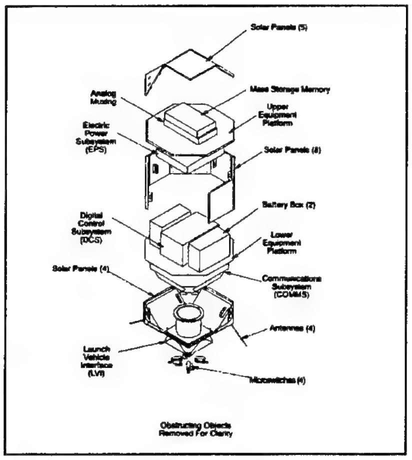


Figure 4. PANSAT Internal Structure [Ref. 1]

b. Electrical Power Subsystem (EPS)

The electronic subsystems are functionally linked as depicted in the PANSAT functional block diagram (Fig. 5).

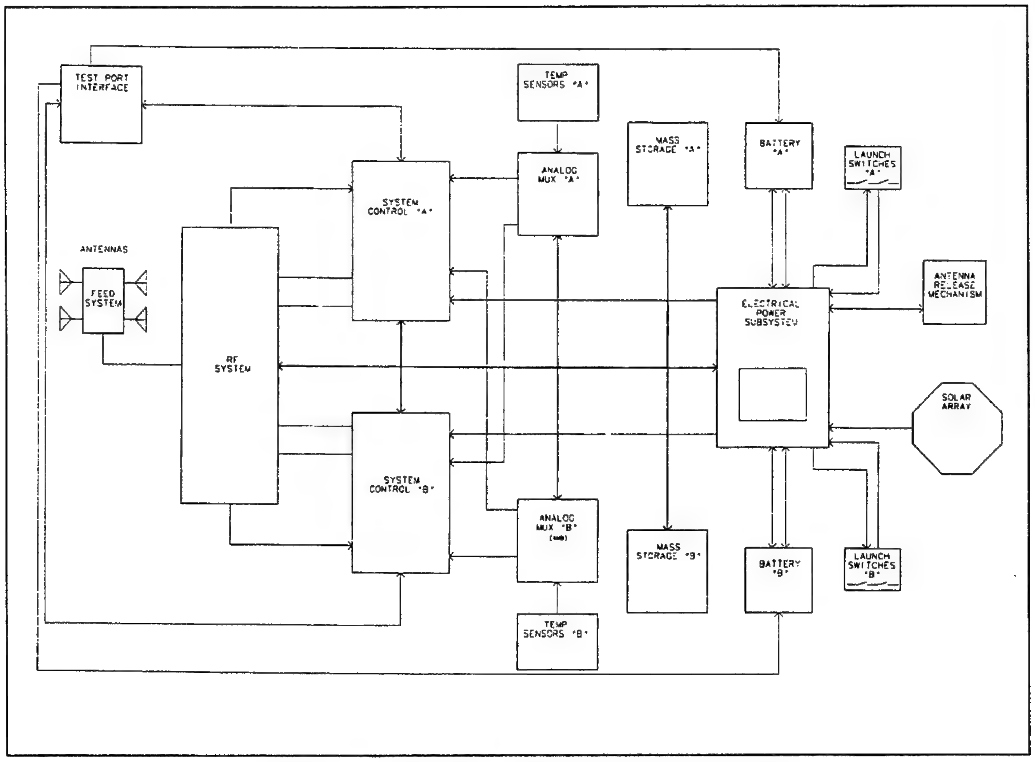


Figure 5. PANSAT Functional Block Diagram

Consisting of two major functional divisions, logic control and power distribution, the EPS is responsible for generating and disseminating all electrical power used throughout the spacecraft. The EPS functional block diagram is shown in (Fig. 6).

Logic control of the EPS provides the necessary internal command and control interface with the digital control subsystem (DCS) for the distribution of power within the S/C. It also retains the capability to reinitialize the S/C in the event of a DCS failure. The reinitializing component of the EPS architecture is called the watchdog timer (WDT). The WDT is nothing more than a timing circuit, which is periodically reset by a signal from the DCS. This signal provides the WDT with the operational status of the DCS. If the WDT has not been reset after a given period of time, then the WDT will assume the DCS has failed and cause power to be applied to the redundant DCS. This will in turn cause the S/C to begin initialization procedures. The WDT (Fig. A.3) does this operation by causing the D flip-flop, U27:A, to change state which triggers a signal to close the respective switch (Fig. A.1 and A.5), either S7 or S8, which applies power to the redundant DCS and commences initialization procedures.

The remainder of the EPS logic board provides an interface with the peripheral control bus (PCB) that allows the PCB to control EPS status measurements. The following measurements go directly to an analog input in the DCS:

(1) Battery cell voltage monitoring

(2) Battery current monitoring

(3) Solar panel current monitoring

(4) Total bus current

(5) Raw bus voltage

(6) Power switch control

(7) WDT reset

Primary electrical power is supplied by 17 solar panels (256 cm^2 per panel). The panels are connected in parallel to the EPS raw bus. Each panel is double wired and fused on the power line at both the solar panel and the EPS bus connection, to increase the power source reliability. Blocking diodes from each panel prevent reverse current flow through a low power panel which would act as an energy sink and may cause panel damage. Each panel consists of one string containing 32 series connected silicon (Si) cells, each cell being 2 cm by 4 cm in size.

During orbit eclipse periods, power is supplied from the secondary source of power, one of the two Nickel Cadmium (Ni-Cd) batteries, to maintain the bus voltage at 12 ±3 Vdc. Each of the batteries contain 10 type D cells connected in series. Space qualified batteries will not be employed due to their prohibitive cost. The use of terrestrial batteries will be of beneficial experimental value for a S/C deployed in low earth orbit. Extensive battery testing is in progress to determine operational characteristics and parameters.

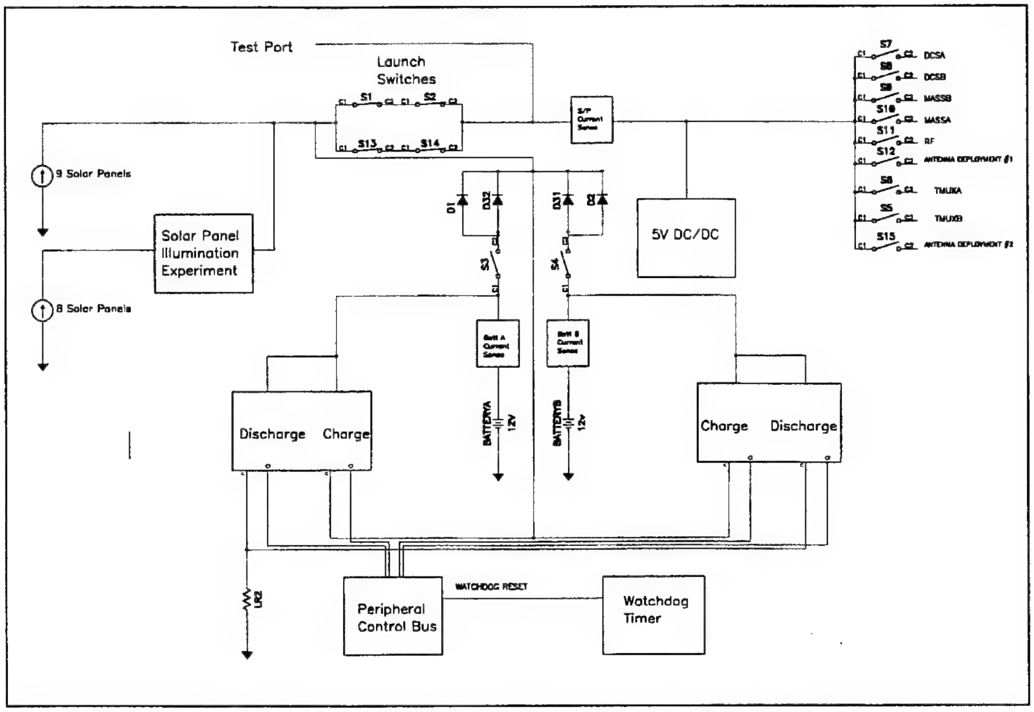


Figure 6. PANSAT EPS Functional Block Diagram

Power from the energy sources is isolated from distribution to the rest of the S/C by the use of mechanical launch switches. These switches, closed upon ejection from the shuttle, are a safety feature required by NASA to prevent accidental radiation of energy by the S/C until after it has been deployed from the shuttle cargo bay. Two sets of switches , connected in parallel, are employed to increase switch operation (closure) reliability.

Raw bus power (9 to 15 Vdc) to the various subsystems is controlled by electronic switching circuits, S5 through S15, to provide power to the DCS, Mass Storage (MASS), radio frequency (RF), Temperature Multiplexing (TMUX), and antenna deployment circuits. Each switch, with the exception of the RF, is fused to prevent a circuit failure in one switch or subsystem from being reflected throughout the EPS distribution and cause a catastrophic failure. The RF switch is not fused, since the RF system contains some level of redundancy. A catastrophic failure in the RF subsystem will cause a critical failure regardless, and it is not desirable to deploy a system where one faulty fuse could cause a critical failure of the system. Each switch, with the exception of the DCS power switches, is controlled by a signal from the DCS to the EPS via the PCB. The DCS power switches, as previously mentioned, are controlled internal to the EPS by the WDT.

c. Thermal Control

The PANSAT design is unique in that it possesses no active thermal control devices. Preliminary thermal analysis have concluded that the passive thermal design system will maintain the components within their required limits. Various temperature sensors are mounted throughout the S/C to provide warnings and status and are included as part of the telemetry data. Only the battery temperature sensors will perform any active role, being used by the battery monitor program to determine and monitor battery state of charge, particularly during charging operations. The various analog temperature data points are multiplexed with the TMUX circuitry and passed to the DCS as analog signals. Each analog signal is converted to digital format via analog to digital (A/D) converters within the DCS and stored in the mass storage devices as historical telemetry data.

d. Digital Control Subsystem (DCS)

The DCS coordinates the operations of the EPS, RF communication suite, and other mission essential operations like health and welfare monitoring. The DCS consists of three principal modules: system controllers (SC), analog mulitplexers (MUX), and mass storage (MASS) devices. Redundant modules, designated A and B, are provided for each function.

The compact design of the PANSAT structure necessitated a minimum quantity of interconnecting cabling within the S/C. The PCB provides a medium to distribute power to the various subsystems as well as a command and data signaling bus for the

DCS to control and monitor the S/C. Communication data, temperature monitoring data, and power sensing data are also passed on the PCB making it a vital link for all operations. This fact alone makes it a extremely important component, especially from a reliability viewpoint, since one wire break can cause a critical failure of the system.

The SC is the hub from which all S/C operations are controlled. There are two printed circuit boards which comprise the SC module (Fig. 7), the DCS digital board and the modem board which is commonly referred to as the PARAMAX module. Each DCS digital board contains:

1. Microprocessor (μP)

2. A/D converters (for multiplexed temperature, current, voltage measurements)

3. PCB interface

4. Error detection and correction (EDAC) for μP random access memory (RAM)

5. Serial communications controller (SCC) for the modem

6. Programmable read only memory (PROM)

The modem board is responsible for interfacing the digital data stream (i.e., message traffic) between the μP (via the SCC) and the RF communication suite. The modulated intermediate frequency (IF) signal at 70 MHz is an input (output) from (to) the RF subsystem. The modem conducts A/D conversion (as required) and demodulation (and modulation) of the message. The signal is spread (and despread) using a pseudo noise (PN) code generator.

Analog multiplexers on the DCS provide A/D conversion of temperature sensor data for telemetry monitoring and archiving in the MASS devices. This data is used for historical health and welfare monitoring by the NPS ground station and is included in the down-linked telemetry message.

There are two redundant mass storage devices (MASS A and MASS B), each of which contain 4 megabytes of volatile static RAM as well as 512 kilobytes of non-volatile flash memory. The non-volatile memory is not space qualified (non-radiation hardened) and is being flown on an experimental basis. The flash memory will not be relied upon to maintain any required software programs or message traffic, but will be used on an experimental basis to build a data base for future exploitation.

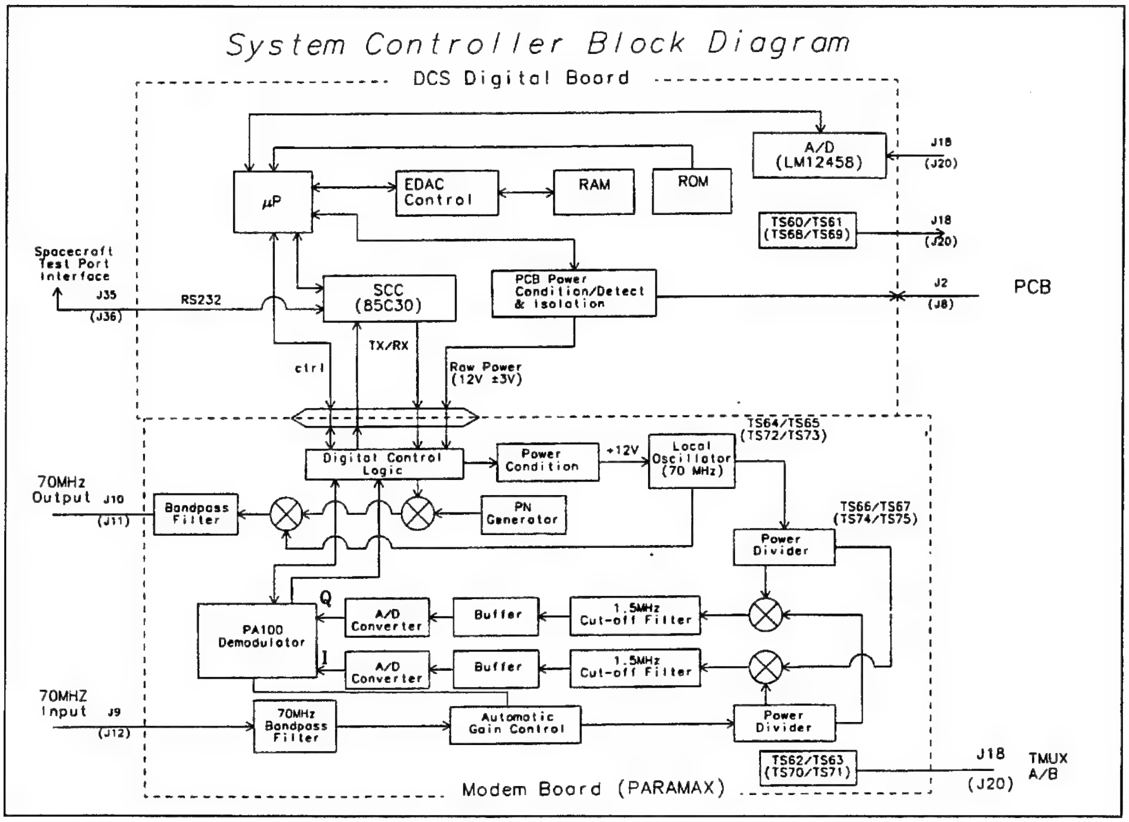


Figure 7. PANSAT System Controller Block Diagram

e. Communication (COMM) Subsystem

The PANSAT communication subsystem (Fig. 8) is the only spacecraft payload . Predominantly referenced as the RF subsystem, it will operate in the amateur radio community 70 centimeter wavelength band providing digital radio packet switching communication using direct spread spectrum techniques. The RF section is located on the lower equipment plate. It includes frequency conversion, low noise amplification (LNA), high power amplification (HPA), and raw bus power conditioning.

(1) Reception. The received signal from the antenna system is routed to the receiver section by the transmit/receive switch (T/R) shown in fig. 8 as S1. The signal is then routed to one of the two low noise amplifier (LNA) circuits by the signal routing switch (S2). Frequency down shift to the 70 MHz intermediate frequency (IF) is performed by one of two signal mixers. The IF signal, still in DSSS format, is routed to the DCS (A or B) modem board where it is processed.

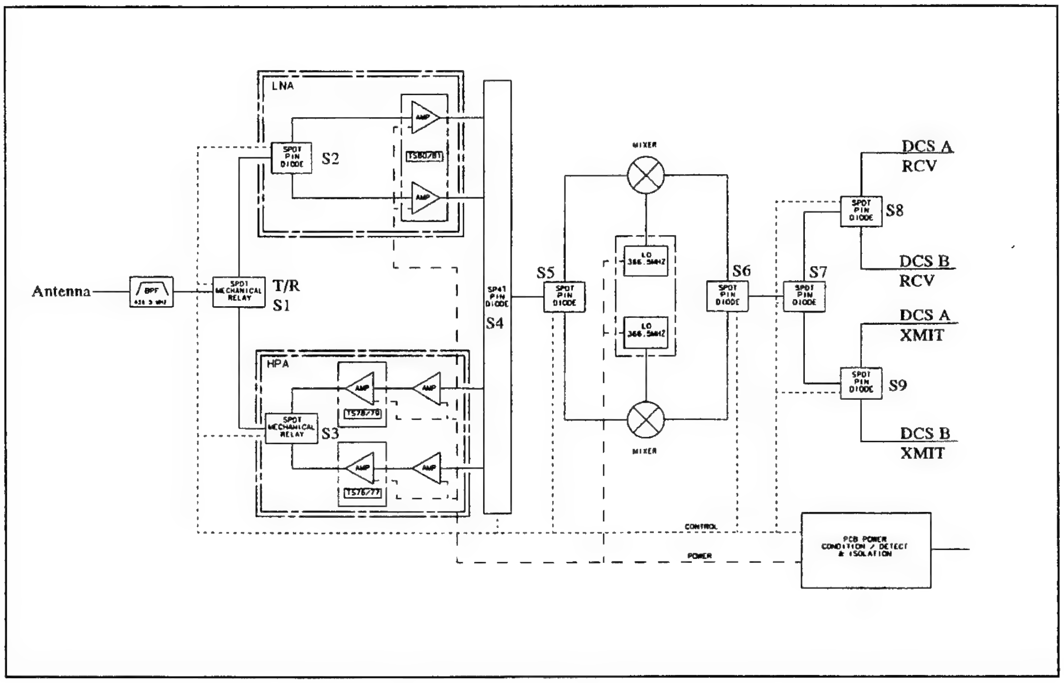


Figure 8. RF Subsystem Block Diagram

(2) Transmission. A DSSS signal is routed from one of the DCS modem boards at IF to the common RF transmit switch (S9). The signal is routed to a mixer where it is shifted to transmit frequency of 366.5 MHz. Amplification of the signal is conducted by one of two high power amplifiers (HPA). Each HPA is composed of two cascaded amplifiers. The transmit signal is then routed to the antenna via the T/R switch.

The antenna element consist of 4 dipole antennas in a tangential turnstile configuration mounted on the bottom half of the S/C (Fig. 3). The feed system connects the four antennas and performs impedance matching between the antenna and the coaxial cable connecting the feed system to the band pass filter.

Functional redundancy is built within the RF subsystem, with the exception of 9 DCS commanded switches or relays used to route the receive and transmit signals.

2. Software Architecture

The computer system architecture employed by the PANSAT design may best be described as a model which incorporates both the software and hardware layers. Software tasks, which provide the user services, are placed on top the architectural hierarchy with protocol handlers (i.e., the operating system) and hardware structure as lower layers. Figure 9 demonstrates the hierarchy of the hardware communications equipment, operating system, protocol software and other software tasks for the S/C.

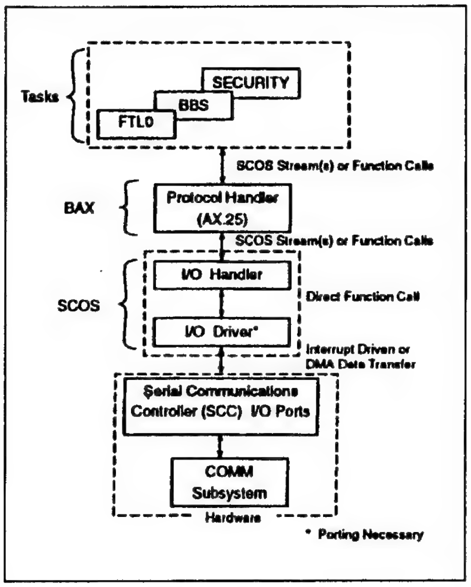

Tasks
SECURITY
BBS
FTL0
SCOS Stream(s) or Function Calls
BAX
Protocol Handler (AX.25)
SCOS Stream(s) or Function Calls
SCOS
I/O Handler
Direct Function Call
I/O Driver*
Interrupt Driven or DMA Data Transfer
Serial Communications Controller (SCC) I/O Ports
COMM Subsystem
Hardware
* Porting Necessary

Figure 9. PANSAT Computer Architecture [Ref. 3]

a. Operating system structure

The PANSAT architecture will take advantage of two proven commercial software products, the Space Craft Operating System (SCOS) and a companion product called BekTek AX.25 (BAX) which implements the link layer protocol. The SCOS will provide a standard application program interface to assist in the development of multi-tasking applications. These services include a real-time multi-tasking kernel, message passing facilities for inter-task communications, Direct Memory Access (DMA), and interrupt driven Input/Output (I/O) drivers.

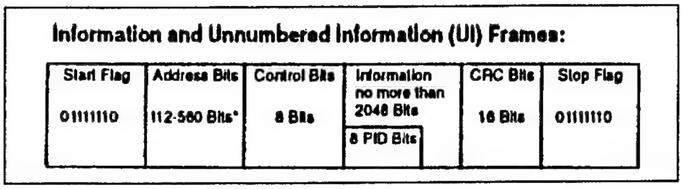
Post launch modification of the software structure is a design requirement that will considerably enhance the functionality and reliability of the software environment. The experimental nature of the S/C does not permit an encompassing forecast of the S/C operating scenarios during the design process.

The boot process will consist of the minimum actions required to initialize the necessary hardware so that the S/C is capable of communicating with the ground station. This will allow the capability to upload any software component, including the operating system.

b. Link layered protocol

Amateur packet radio is a communication technique that allows high speed and low error rate digital data exchange. A data link protocol was developed by the amateur radio community that is compatible with the seven layer Open Systems Interconnection (OSI) reference model. This protocol, called AX.25, was adopted by the amateur radio community as a offshoot of the International Telegraph and Telephone Consultative Committee (CCITT) X.25 data link layer protocol, a standard for packet switching.

The data link layer, considered the second level protocol, provides the communication between physical layer (modem) with the network layer. For this design, this is basically the application programs. This is accomplished by receiving streams of bits from the physical layer and applying a structure, or frame, to those streams (Fig. 10). Each frame is composed of several smaller groups of data, called fields, which are used for various overhead data management and the raw data information. The AX.25 protocol uses a technique called bit stuffing which is used to maintain a unique bit pattern sequencing within a frame and eliminate the possibility of flags appearing within the contents of a frame. Error detection of each frame, or cyclic redundancy checks (CRC), helps detect any corruption of data by the physical layer.



Information and Unnumbered Information (UI) Frames:

Start Flag	Address Bits	Control Bits	Information no more than 2048 Bits	CRC Bits	Stop Flag
01111110	112-560 Bits*	8 Bits	8 PID Bits	16 Bits	01111110

Figure 10. AX.25 Information Frame [Ref. 3]

The AX.25 frame management scheme allows the information to be sent in packets, with up to eight outstanding frames in a relay sequence [Ref. 3]. Burst transmissions of these frames will allow multiple users in the same geographical area to access the S/C on a single pass. There are other small satellites deployed which possess this capability for packet switching, but none that have attempted to do it utilizing spread spectrum modulation techniques.

c. *Spacecraft Commanding*

Commanding of the S/C is required for software program uploads and other subsystem command functions. These command functions can include routine operations such as battery charging, battery reconditioning, and transmitter power level modifications. Commanding may also be necessary to reconfigure the system due to a failure, abnormal operation, or impending failure conditions.

3. Ground Station

A ground station is required to conduct S/C management, maintenance control, and data archiving. The ground station, located at NPS and administered by the Space Systems Academic Group (SSAG), will be the focal point for S/C commanding, software system uploads, health and welfare data collection, archiving, and will provide an external interface with the amateur radio community. This external interface, as presently planned, will be via the Internet with a dedicated world wide web (www) home page for the PANSAT program. This will provide the user not only the capability to obtain necessary access data such as orbital ephimerus, transmission frequency, S/C availability, and the PN code for spread spectrum operations, but also interesting program data such as user statistics and archived telemetry data.

C. PROGRAM LIFE-CYCLE

The PANSAT project has evolved from conception in 1989 to it's present design state . As depicted in Fig. 11, a subsystem design freeze in late 1995 will be made to support a STS-86 Atlantis launch in late 1997.

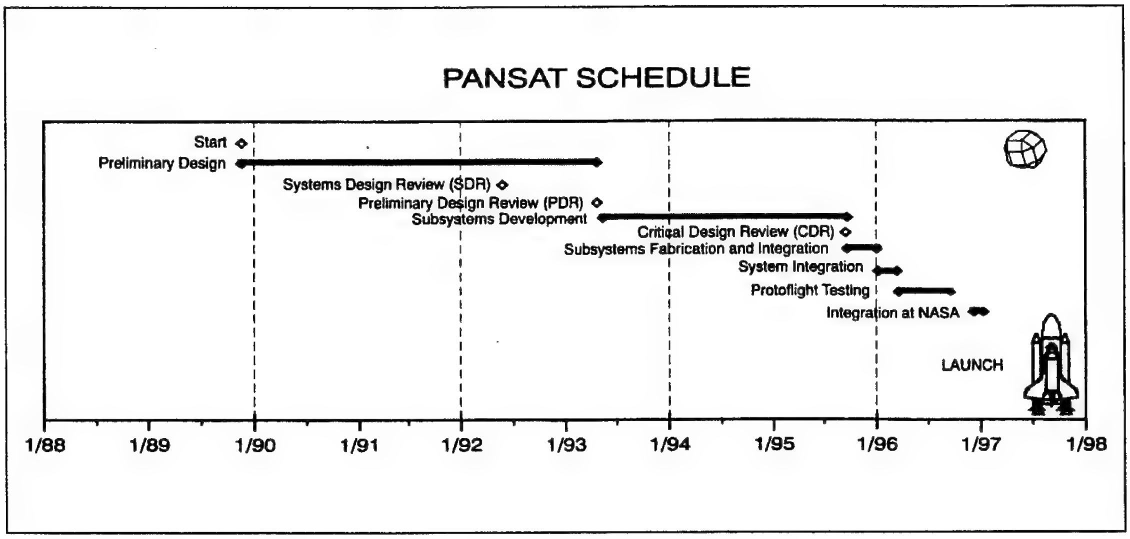


Figure 11. PANSAT Design Life-cycle

1. Mission Duration

The present launch scenario from the shuttle, would give the S/C an orbit life of approximately two years before it decays into the earth's atmosphere. Other launch options, including various shuttle orbits, are being investigated as possible launch scenarios. Regardless of the launch scenario, a two year mean mission duration requirement is maintained for the S/C hardware architecture.

2. Launch Options

a. Hitchhiker Program

The PANSAT S/C can be launched from a Shuttle Get Away Special (GAS) canister as a payload of the hitchhiker program. The S/C is mounted in a GAS canister in the shuttle's cargo bay by a marman clamp from an ejection mechanism to the S/C LVI.

No other interface between the S/C and the shuttle is required. All commanding and control of the S/C will be made by the NPS ground station once the S/C is deployed and initialized.

b. Minuteman

Launch from a refurbished minuteman launch vehicle is a recent option available for spacecraft desiring a LEO. Capable of placing PANSAT in a much higher orbit and inclination, it radically modifies the orbital and mission options. Able to place the S/C in sun-synchronous orbit, it could modify the deployment requirements of a power conscious design such as PANSAT or a follow-on project.

III. RELIABILITY

A. RELIABILITY ANALYSIS BACKGROUND

The political climate in today's marketplace, both government and industrial, does not afford the decision maker the luxury of balloon budgets and long production lead times. Social, political, and economic constraints dictate the exploitation of alternative methods to maximize the efficiency and effectiveness of every system produced. The goal of reliability analysis thus becomes a technique to measure and enhance the systems reliability at minimum cost. This will permit program managers and system designers to deploy the most cost effective system.

1. Stages of Systems Analysis

There are two avenues of thought process which encompass system reliability analysis. These processes are inductive and deductive reasoning [Ref. 4]. The two processes may be unique to a particular analysis method or stage in the analysis procedure.

a. Inductive

During the inductive stage, information is researched, gathered, and organized to conceptualize the systems definition, functional description, and determination of the critical components. This process helps to answer the question "***What can happen to the system as a result of a component failure or human error?***".

b. Deductive

The deductive analysis of a system design helps answer the question "***How can the system fail?***". A logic tree is often the best device for deducing how a major system failure event could occur. Application of such a method requires an in-depth understanding of how the system operates within the operational environment. Many methods of analysis are available for performing the analysis, such as fault tree analysis, decomposition, circuit stress analysis, or the state space approach. Each application may be more suitable at various stages of the program life-cycle. Fault tree analysis (FTA) was chosen for PANSAT hardware design analysis due to the applicability of the process to the design status. The use of FTA can be very beneficial as a design tool to identify potential flaws in a system design and help eliminate costly design changes and retrofits. Equally valuable as a diagnostic tool, it can predict the mostly likely causes of a system failure.

2. Phased Mission Profiles

The various mission profiles of spacecraft (S/C) operation have distinct effects on system reliability. A mission phase is defined as a period of time in which the functional organization of the system is constant. The system must accomplish a specific task, or set of tasks, during each particular phase. Detailed analysis of a system must be accomplished independently for each phase of the mission life-cycle.

Due to the simplistic operational profile of the PANSAT S/C, due largely to the absence of any attitude control or orbital plane change requirements, the life-cycle mission can be reduced into two basic mission phases, launch/initialization and operations.

a. Launch and Initialization

This phase begins immediately upon deployment of the S/C from the GAS canister. During this phase the S/C powers up subsequent to a successful deployment, and when in "daylight" (design analysis assumes dead batteries upon launch) conducts hardware and basic operating system initialization procedures which include:

(1) Hardware diagnostics which test for failure conditions and configure the S/C accordingly. Diagnostic procedures are continuously performed if the S/C has failed to acquire communications with the NPS ground station.

(2) A basic operating system is loaded from onboard ROM storage. This system contains the basic command list for the higher level operating system . The higher

level operating system and application software is uploaded from the NPS ground station once the communication link has been established and the S/C is in a stable configuration.

(3) It is anticipated that both onboard storage batteries will be depleted upon ejection from the shuttle. An initialization procedure will require at least one of the batteries to be charged to an acceptable level prior to any interaction of the S/C with a ground station.

(4) The four dipole antennas are tied back in a stowed condition while the S/C is in the GAS canister. Upon ejection from the canister the antennas will be deployed by burning the nylon restraints with heaters powered by the solar arrays.

(5) Link closure with the NPS ground station is the final objective for the initialization segment. If satisfactory conditions are present, the high level operating system and application software will be up loaded to the S/C.

The launch and initialization phase could last several days before the link with NPS has been established. Following software uploads the S/C will undergo a testing period.

b. Operations

This phase is the normal operating mode of the S/C. The S/C enters this phase once the preceding phase is completed satisfactorily. The analysis of this thesis will concentrate on this phase, assuming initialization phase has occurred without incident.

B. FAULT TREE ANALYSIS DESCRIPTION

It is beneficial to understand the background of FTA to gain a better appreciation of the basis, application, and limitations of the method. As a visual tool it is useful in communicating and supporting decisions based upon the analysis, both for the design engineer and the management decision maker. Fault tree analysis also provides a convenient and efficient format that is helpful for both qualitative and quantitative evaluation [Ref. 4].

1. Historical Background

Conceived by H. A. Watson of the Bell Telephone Laboratories in 1961 to evaluate the safety of the Minuteman ICBM launch control system, the method has evolved into one of the most powerful analytical tools used to evaluate system safety [Ref. 5]. As the method has developed, its application to solving real world analysis problems has also expanded. Once a tedious procedure requiring large analytical teams, it can now be performed by a single reliability analyst using powerful reliability software tools. The application of FTA has spread from humble beginnings in the aerospace industry to vast commercial applications, including its use as the principal method for system safety analysis (hazard analysis) in the nuclear power industry.

2. Fault Tree Analysis Utility

Events or situations requiring the application of FTA are typically identified by inductive analysis or system analyst intuition. Typically the events are the result of some subsystem functional failure. The method is unusually versatile in that it permits sensitivity analysis, analysis qualification, analysis quantification, and evaluation of alternative designs for potential tradeoffs. The FTA method is unique in that it also can be used to create a success tree.

a. Advantages

The FTA method has four major advantages over other forms of systems critical failure analysis [Ref. 5].

(1) Directs the analyst deductively to accident related events. The deductive approach to describing how a system could fail, often referred to as the top-down approach, will uncover all failures or combinations thereof which could cause the undesired event. This kind of approach lends itself to better organization and control than other methods based on a bottom-up approach.

(2) Provides depiction of system functions that lead to undesired outcomes. The graphical representation of the fault tree provides the decision maker with a clear and concise understanding of the inter-relationship of failure events.

(3) Provides options for both qualitative and quantitative analysis. Quantitative analysis is desirable if solid reliability data is available for the tree's end events. Quantification permits the measurement of the likelihood of occurrence of the top event, node, or subsystem within the tree. Probabilistic measures of importance (i.e., reliability importance) can be obtained and an objective measure of the risk can be ascertained utilizing this approach.

Early in the development cycle reliability data may not be available due to either insufficient reliability data on the components or the maturity of the design. Qualitative analysis, however, can provide the failure event sets and measures of the importance of the individual end events in the causation process. Qualitative analysis is more commonly used because it does not require precise failure rates for the end events. It results in sets of events that cause the top event and a ranking of these events for their importance in causing the top event. This relationship is known as the systems structural importance.

(4) Provides analyst with insight into system behavior. The process of FTA is so detailed in its logical relationships, that it forces the analyst to understand the system beyond the level enjoyed by even some subsystem design engineers or system managers.

b. Disadvantages

The significant shortcomings of FTA, that may be of any consequence, relate to the process of synthesizing a fault tree. Often time consuming and overwhelming in detail, even for designs as simple as PANSAT, can require considerable effort to embrace a comprehensive study of all the common cause failures. Failure mode oversight and omission may be one of the major drawbacks to FTA, but this is true for any analysis methodology.

Modeling of the fault tree may be difficult when attempting to describe the failure of system components that can operate in a degraded mode. The Boolean logic structure of the fault tree assumes a component is either working or has failed. This fact limits FTA process to analyzing the system for critical failures only.

Despite its drawbacks, as systems become increasingly more complex, the deductive and systematic approach used by FTA becomes increasingly beneficial. The increased availability of low cost software packages has been an overwhelming aid in constructing and analyzing fault trees, making the effort not only beneficial but time and cost efficient as well.

c. Assumptions

Similar to all forms of analysis methods, FTA is restricted to the domain constraints for which it is valid. The following assumptions were made to assist in the synthesis of the fault tree.

(1) The composition of fault tree assumes components are capable of only two states of performance, either functioning or failed. The probability the component is functioning at some time *t* may be characterized by some statistical distribution. The exponential distribution is often chosen for components exhibiting constant, or nearly constant, failure rates. As with the components, the system is dependent upon the performance of it's components and is capable of only obtaining two states of performance, functioning or failed.

(2) Each of the systems components is assumed to have statistically independent lives. There is no ability to repair or replace any component, and each embraces a finite lifetime.

(3) The S/C physical structure is assumed to remain intact for the duration of its mission. Although it will undergo stress and strains, particularly during launch, it is assumed that it will never operate outside it's design envelope. No structural component

will experience strains greater than the elastic limit nor fatigue failure due to mechanical and thermal cycling.

(4) Each component in the fault tree is relevant to the systems operation. This infers that each basic event appears in at least one of the minimum cut sets. A minimum cut set is defined as combination of the fewest component failures that cause the system to fail. Complex systems my have a large number of minimum cut sets.

C. THEORETICAL DEVELOPMENT

System structures are based on two generic structures. These are the series and the parallel structured systems. The series system functions if all of it's components function, and the parallel system functions if at least one of it's components function (Fig. 12). The relationship of the performance of the components to the performance of the system defines the performance logic of the system. Fault tree analysis will correlate the functional block diagram of the system structure to the logic structure of the system. The following background will illustrate the development of FTA theory, and insures essential issues are addressed in the synthesis of the fault tree. The vast majority of the following theoretical derivation was taken from Professor J.D. Esary notes [Ref. 6] and notes from a reliability course [Ref. 7].

1. Structure Function

The structure function, $\Phi(\mathbf{x})$, for a system relates the operation of a system's components to the operation of the system. There are many analytical advantages to the derivation of the structure function as will be evident later.

a. Notation

(1) All vectors are represented in bold case type

(2) T is the time to system failure

(3) T_i is the time to component i failure

(4) x_i is a Binomial random variable (r.v.) of the component i with value

$$x_i = \left\{ \begin{array}{l} 1 \text{ if component i is functioning} \\ 0 \text{ if component i has failed} \end{array} \right\}$$

(5) $\mathbf{x} = \{x_1, x_2, ..., x_n\}$ is the system state vector in which n components describe the system structure.

(6) $P[x_i=1] = p_i$ is the probability of component i working at some time *t*

(7) $P[x_i=0] = 1-p_i$ is the probability component i has failed by time *t*

(8) $\mathbf{p} = \{p_1, p_2, ..., p_n\}$ is the system probability vector

(9) $E[\mathbf{y}]$ is the expected value of the r.v. $\mathbf{y}$

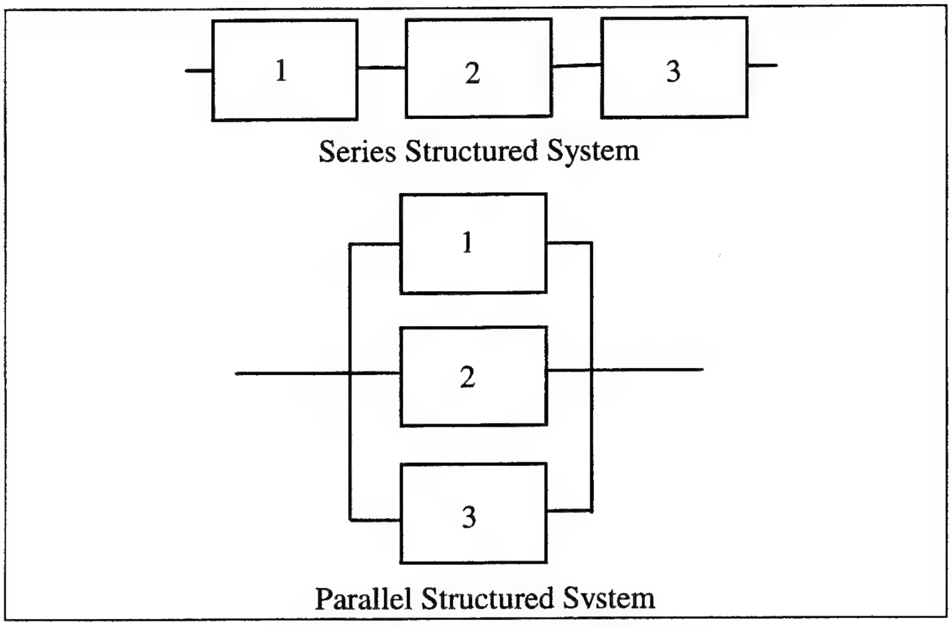


Figure 12. Generic System Structures

(10) $\Phi(\mathbf{x})$ is the system structure function describing the state of the system.

$$\Phi(\mathbf{x}) = \left\{ \begin{array}{l} 1 \text{ if system is working at time t} \\ 0 \text{ otherwise} \end{array} \right\}$$

(11) $\Phi(1_i, \mathbf{x})$ represents the structure function in which the i<u>th</u> component of the state vector $\mathbf{x}$ has the binomial value of one.

(12) $\Phi(0_i, \mathbf{x})$ represents the structure function in which the ith component of the state vector **x** has the binomial value of zero.

(13) Mathematical notation:

$$\prod_{i=1}^{n} x_i = (x_1)(x_2)\cdots(x_n)$$

$$\coprod_{i=1}^{n} x_i = 1 - \prod_{i=1}^{n} (1 - x_i)$$

b. Series Structure

The series structured system (Fig. 12) demands each component to function in order for the system to function. If any component were to fail then the system would subsequently fail. The system lifetime is therefore dependent upon the weakest link, or the shortest component lifetime. The system structure function for a series structured system is shown in eq. 1 as the multiplication of all the component binomial states.

$$P[T \geq t] = P[\min(T_1, T_2, \cdots, T_n) \geq t]$$

$$\Phi(\mathbf{x}) = \left\{ \begin{array}{l} 1 \text{ iff } x_i = 1;\ i = 1, 2, \cdots, n \\ 0 \text{ if any } x_i = 0 \end{array} \right\}$$

$$= \prod_{i=1}^{n} x_i \tag{1}$$

c. Parallel Structure

The parallel structured system (Fig. 12) only requires at least one of the parallel component's operation in order for the system to operate. If all the components in parallel were to fail then the system would system fail. The system lifetime is therefore dependent upon the longest component lifetime. Equation 2 demonstrates how the parallel system structure function is determined. A simple example at the conclusion of this chapter provides insight for the application of this mathematical notation.

$$P[T \geq t] = P[\max(T_1, T_2, \cdots, T_n) \geq t]$$

$$\Phi(\mathbf{x}) = \left\{ \begin{array}{l} 1 \text{ if any } x_i{=}1;\ i{=}1, 2, \cdots, n \\ 0 \text{ iff all } x_i{=}0;\ i{=}1, 2, \cdots, n \end{array} \right\}$$

$$= \coprod_{i=1}^{n} x_i = 1 - \prod_{i=1}^{n} (1 - x_i) = x_1 \coprod x_2 \coprod \cdots \coprod x_n \tag{2}$$

2. Component Relevance

A component is relevant to the systems operation if it's failure can affect the performance of the system, and should be considered when conducting the failure analysis. If component i is relevant to the systems operation then eq. 3 is true.

$$\Phi(1_i, \mathbf{x}) \neq \Phi(0_i, \mathbf{x}) \ \forall \ (\cdot_i\, , \ \mathbf{x}) \tag{3}$$

Conversely if a component is irrelevant it's operation has no influence on the function of the system, and the condition of eq. 4 is always true.

$$\Phi(1_i, \mathbf{x}) = \Phi(0_i, \mathbf{x}) \ \forall \ \mathbf{x} \tag{4}$$

The concept of relevance is important when determining the reliability function of the system. Only components relevant to the system operation should be considered when determining the reliability of the system. An importance consideration in defining component relevance therefore becomes one of defining what constitutes the systems operational status.

3. Coherent Systems

A system is defined as a coherent system if it's structure function satisfies the following three conditions.

a. $\Phi(\mathbf{1}) = 1$ where **1** is the vector (1, 1, ..., 1)

b. $\Phi(\mathbf{0}) = 0$ where **0** is the vector (0, 0, ..., 0)

c. $\Phi(\mathbf{x}) \leq \Phi(\mathbf{y})$ whenever $x_i \leq y_i \ \forall i$

A coherent structure is monotonic non-decreasing in **x** and all structure components are relevant to the systems operation. Many times the structure function is not easily defined, but can be approximated by bounding the function. The structure function can always be bounded below by the series structured case and bounded above by the parallel structured case as shown with eq. 5. The loose bounds inherent to eq. 5 may limit it's practical use.

(5)
$$\prod_{i=1}^{n} x_i \le \Phi(\mathbf{x}) \le \coprod_{i=1}^{n} x_i$$

4. Minimal Path and Minimal Cut Sets

a. Minimal Path Sets

A path set of a coherent system is the set of components, which by all working, cause the system to function. The minimal path set is the smallest subset of components within the path set which by all working cause the system to function. The union of all minimum path sets then define the set of system relevant components. Using vector notation for the system of components, a path set would be the combination of set **x** components that satisfy:

(6)
$$\Phi(\mathbf{x}) = 1 \text{ (i.e., system working)}$$

Let ρ_j describe the j<u>th</u> minimum path set (p possible minimum path sets) where $\rho_j(\mathbf{x})$ is a binary function. Since all components of a minimum path set must function for the system to function, the minimum path set is similar to the series system structure. Equation 7 defines the structure of the minimum path set function.

(7)
$$\rho_j(\mathbf{x}) = \prod_{i \in \rho_j} x_i = \left\{ \begin{array}{l} 1 \text{ if all } x_i \text{ working} \\ 0 \text{ otherwise} \end{array} \right\}$$

Only one minimum path set must function for the system to function. The parallel arrangement of minimum path sets can therefore describe the systems structural relationship. Equation 8 describes the system structure function using the minimum path set notation. Figure 13 shows a pictorial relationship for the minimum path sets for an example problem.

$$\Phi(\mathbf{x}) = \coprod_{j=1}^{n} \rho_j(\mathbf{x}) \tag{8}$$

The structure function can then be viewed as a parallel arrangement of the path sets. This is typically referenced as a parallel-series arrangement.

b. Minimum Cut Sets

A cut set of a system's structure refers to a combination of component failures that would cause the systems failure. The minimum cut set is therefore the smallest subset of components which by all failing cause the system to fail. Analysis of minimum cut sets are an important aspect of FTA from a qualitative standpoint. Similarly to the path set notation, a cut set is one that satisfies eq. 9.

$$\Phi(\mathbf{x}) = 0 \text{ (i.e., system failed)} \tag{9}$$

Let κ_j be the jth minimum cut set (k possible minimum cut sets) where $\kappa_j(\mathbf{x})$ is a binary function. All the components in a minimum cut set must fail to cause the system to fail. This is similar to a parallel structured system. Equation 10 defines the minimum cut set function.

$$\kappa_j(\mathbf{x}) = \coprod_{i \in \kappa_j} x_i = \left\{ \begin{array}{l} 0 \text{ iff all } x_i \text{ in the cut set have failed} \\ 1 \text{ otherwise} \end{array} \right\} \tag{10}$$

Only one minimum cut set must fail to cause the system to fail. The series arrangement of cut sets can therefore describe the systems structural relationship. Equation 11 describes the system structure function using the minimum cut set notation. Figure 13 shows a pictorial relationship for the minimum cut sets for an example problem.

(11) $$\Phi(\mathbf{x}) = \prod_{j=1}^{n} \kappa_j(\mathbf{x})$$

The system will fail if at least one of the κ_j fail. The structure function is referenced in this case as a series arrangement of cut sets. This is typically referenced as a series-parallel arrangement.

5. Importance

It is often productive to gain an insight to a component's importance to the systems operation while conducting systems analysis. Qualitative analysis can provide information to measure a component's importance to the system structure, which in turn can direct design efforts to minimize the failure condition. Once such tools, called structural importance, can play an effective role in the analytical procedure. The component x_i is said to be structurally important the condition of eq. 12 is true.

(12) $$\Phi(1_i, \mathbf{x}) - \Phi(0_i, \mathbf{x}) = 1$$

The components operation is important for the systems operation for a given system state vector **x**. The frequency for which eq. 12 holds true (for every state value of the vector **x**) will determine the structural importance of the component. For example, if a component is listed in 1000 minimum cut sets it would have a higher structural importance than a component that is listed in only 10 minimum cut sets. A parallel argument using path sets can also be made. A meaningful measure of a component's structural importance would be to count how many times eq. 12 holds true for the system structure. Equation 13 defines this frequency of occurrence.

(13)
$$n_{\Phi}(i) = \sum_{\mathbf{x}|x_i=1} [\Phi(1_i,\mathbf{x}) - \Phi(0_i,\mathbf{x})] \quad \textit{(n is a integer number)}$$

To represent the relative structural importance of component (i) with other components in the structure, the components are normalized by eq. 14 for a system of size *m* relevant components. The term $I_{\Phi}(i)$ is known as the normalized structural importance for the i<u>th</u> component.

(14)
$$I_{\Phi}(i) = \frac{n_{\Phi}(i)}{2^{m-1}}$$

A similar argument can be derived which determines the component's importance from a reliability standpoint. For example, a series component, which is a single point failure component, has a mean time to failure (MTTF) of 10 years may not have a reliability importance as critical to that of two redundant parallel components that have a MTTF of 60 days. To determine a component's reliability importance you must be able to determine reliability data for all the relevant components in the system structure. The determination of reliability importance is shown in eq. 15.

(15)
$$I_h(i) = E[\Phi(1_i,\mathbf{x}) - \Phi(0_i,\mathbf{x})]$$

6. Reliability Function

Given the components in a system operate independently, with Binomial r.v. $\mathbf{x} = (x_1, x_2, ..., x_n)$, then we can describe the reliability of the system with the reliability function h(**p**). Equation 16 describes the formulation of the reliability function.

(16)
$$h(\mathbf{p}) = P[\Phi(\mathbf{x}) = 1] = E[\Phi(\mathbf{x})]$$

This equation holds true only if the x_i's are statistically independent. Using the reliability function, the reliability importance described previously can be simply determined using eq. 17 for each component.

(17)
$$I_h(i) = h(1_i, \mathbf{x}) - h(0_i, \mathbf{x}) = \frac{\partial \mathbf{p}}{\partial p_i}$$

7. Association

The previous reliability discussions have assumed component independence. In real world applications this is not always true and should not be lightly assumed. The independence relationship between components will be replaced with an alternative form, association, which is simply non-negative dependence between the components [Ref. 8]. System components can become positively dependent in various manners. For example, two components located side by side on a printed circuit board are subject to the same operational environment. Environmental conditions that effect one component may also effect the other. This creates a common positive dependence between the components. Random variables $\{x_1, x_2, ..., x_n\}$ are said to be associated if there is non-negative covariance between the random variables. Properties of associated r.v.'s are further explained in Ref. 6.

The components of PANSAT fall into the positive dependence category due to the environmental effects. If the reliability is calculated using independent assumptions then the reliability is underestimated for series structure and overestimated for the parallel structure. The reliability value can be bounded, assuming association, by the series and parallel cases. Assume a system consists of k possible minimum cut sets and p possible minimum path sets, then the following theorem, eq. 18, can be shown [Ref. 6] to bound the system reliability.

(18) $$\prod_{j=1}^{k} P[\kappa_j(\mathbf{x}) = 1] \leq P[\Phi(\mathbf{x}) = 1] \leq \coprod_{j=1}^{p} P[\rho_j(\mathbf{x}) = 1]$$

A tighter bound for the reliability, eq. 19, can be generated by observing the probability values for the minimum cut set and minimum path set functions, and applying the most limiting conditions for upper and lower bounds [Ref. 6].

(19) $$\max_{1 \leq j \leq p} \prod_{i \in \rho_j} p_i \leq P[\Phi(\mathbf{x}) = 1] \leq \min_{1 \leq j \leq k} \coprod_{i \in \rho_j} p_i$$

8. Special Structure System (k-out-of-n)

An offshoot of the parallel structure is a system that works if k-out-of-n components function. A practical application of the k-out-of-n concept to the PANSAT design is the notion of solar panel failure. The system will not fail if one solar panel fails, but is definitely inoperable if all 17 solar panels fail. There is some number, *k*, in which the system remains functional only if at least *k* panels are operable. Solar panel failure is an important concern for PANSAT due to it's operation on a very restrictive power margin.

The simple case, where two out of three components are required to be operational for a system to function, is shown in Fig. 13. The diagram shows representation using the minimum path set approach and the minimum cut set approach. Each path represents the minimum component combinations (i.e., two) for a successful mode of system operation. This is referred to the minimum path set representation of the system structure. Figure 13 also shows the minimum cut set representation, where two component failures will cause the system to fail.

Since this is a parallel system, the minimum path sets are obtained by observing the system functional structure. Any combination of two working components will allow the system to function. Application of eq. 7 to the observed set of minimum path sets (x_1, x_2), (x_1, x_3), and (x_2, x_3) will result in the following .

$$\rho_1 = x_1 x_2 ; \ \rho_2 = x_1 x_3 ; \ \rho_3 = x_2 x_3$$

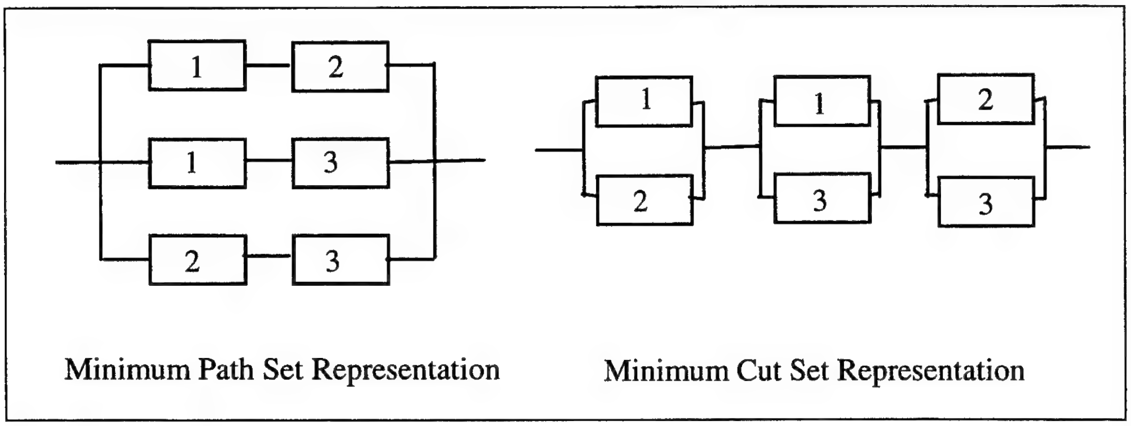
The structure function is determined by applying the minimum path sets to eq. 8.

$$\begin{aligned}
\Phi(\mathbf{x}) = \Phi(x_1, x_2, x_3) &= x_1x_2 \coprod x_1x_2 \coprod x_2x_3 \\
&= x_1x_2 \coprod [1-(1-x_1x_3)(1-x_2x_3)] \\
&= x_1x_2 \coprod [1-(1-x_2x_3-x_1x_3+x_1x_2x_3)] \\
&= x_1x_2 \coprod [x_1x_3+x_2x_3-x_1x_2x_3] \\
&= [1-(1-x_1x_2)(1-(x_1x_3+x_2x_3-x_1x_2x_3))] \\
&= 1-1-x_1x_3-x_2x_3-x_1x_2 \\
&\quad +x_1x_2x_3+x_1x_2x_3+x_1x_2x_3-x_1x_2x_3) \\
&= x_1x_2+x_1x_3+x_2x_3-2x_1x_2x_3
\end{aligned}$$

Since the r.v., x_i , is binomial (i.e., has a value of 0 or 1) the expansion of the above equation is reduced to single order terms by noting the fact that any power of x_i is equal to it's first order value (i.e., $x^p_i = x_i$ for any integer power p). Reduction of the structure function to single order terms is necessary before a one to one correlation of the structure function to the reliability function can be made. Recall the reliability function is only defined for a system of independent components.

An identical system structure solution could be obtained by using the minimum cut set approach. This is demonstrated with an example at the end of the chapter.

The structure function for the k-out-of-n system structure obtains the binomial value shown in eq. 20. A closed form notation of the structure function is not provided here, but the approach is similar to the example shown above.



Minimum Path Set Representation

Minimum Cut Set Representation

Figure 13. Two out of Three Component System

$$\Phi(\mathbf{x}) = \left\{ \begin{array}{l} 1 \text{ if } \sum_{i=1}^{n} x_i \geq k \\ 0 \text{ if } \sum_{i=1}^{n} x_i < k \end{array} \right\} \tag{20}$$

The reliability function, shown in eq. 20, can be described for the k-out-of-n case if the system is configured of identical components and reliability.

$$h(\mathbf{p}) = \sum_{j=k}^{n} \binom{n}{j} p^j (1-p)^{n-j} \tag{21}$$

D. FAULT TREE CONSTRUCTION

The objective of FTA is to model the system conditions that result in an undesirable event under constrained environmental conditions. The fault tree models the various combinations of possible events, both normal and faulty, to give a graphical and logical representation of the systems response resulting in the "Top Event" failure. Setting well defined (yet practical) spatial and temporal bounds on the system is a necessary consideration required of the analyst to ensure the validity of the analysis of a phased system. Figure 14 illustrates the relationship of the system failure (labeled Top Event) to the basic component failures (bottom event or leaves). The conditioning events between the Top event and the fault tree's leaves describe events that could lead to the Top Event. The intermediate events are known as the branches of the fault tree.

1. Methodology

The FTA method structures the relationship of sequential events that lead to an undesired event in a system, to a Boolean logic representation model that reflect the systems functional structure. The top down analysis systematic approach to FTA attempts to define all possible, yet practical, critical failure paths that will cause the Top Event. The fault tree grows downward and outward describing the failures and causes in increasing detail. The fault tree symbology described below represent that used within the FaultrEASE software package [Ref. 9] that was utilized for this analysis.

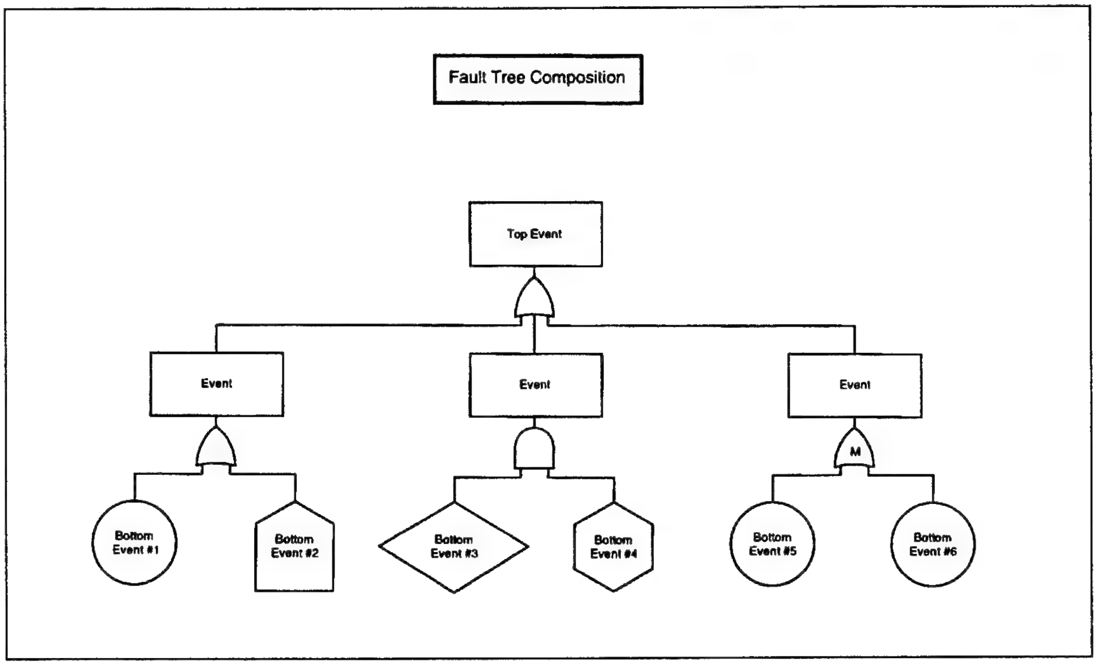


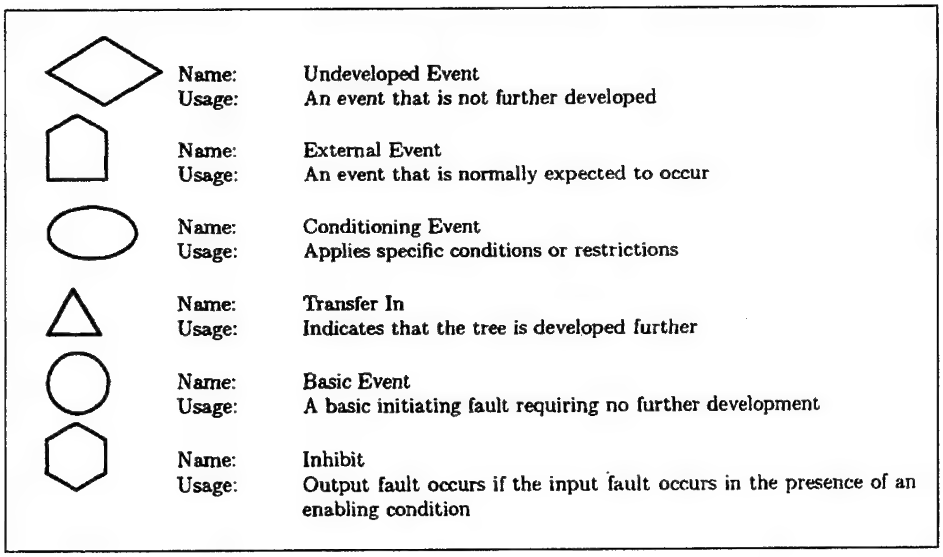
Figure 14. Fault Tree Composition

a. Symbology

(1) Event Symbology. There are various types of failure end events that are represented in the fault tree structure. The synthesis, or structuring, of the events provides a logical fault flow process by combining the system failure events with Boolean logic operators. The respective event symbols (Fig. 15) describe the type of events, and when combined with the logical operators help define a cut set for the Top Event occurrence. End events are referred to as the leaves of the fault tree.

(2) Logic Gate Symbology. The fault tree represents the logical relationship between the events of the system. These relationships can be described using a wide assortment of Boolean logic operators (i.e., Boolean logic gates). The two basic logical relationships used to describe the majority of the fault tree relationships are the logical

"OR" and "AND" operators (Fig. 16). Within the fault tree, a rectangle is placed above each operator to describe the event.



Name: Undeveloped Event
Usage: An event that is not further developed

Name: External Event
Usage: An event that is normally expected to occur

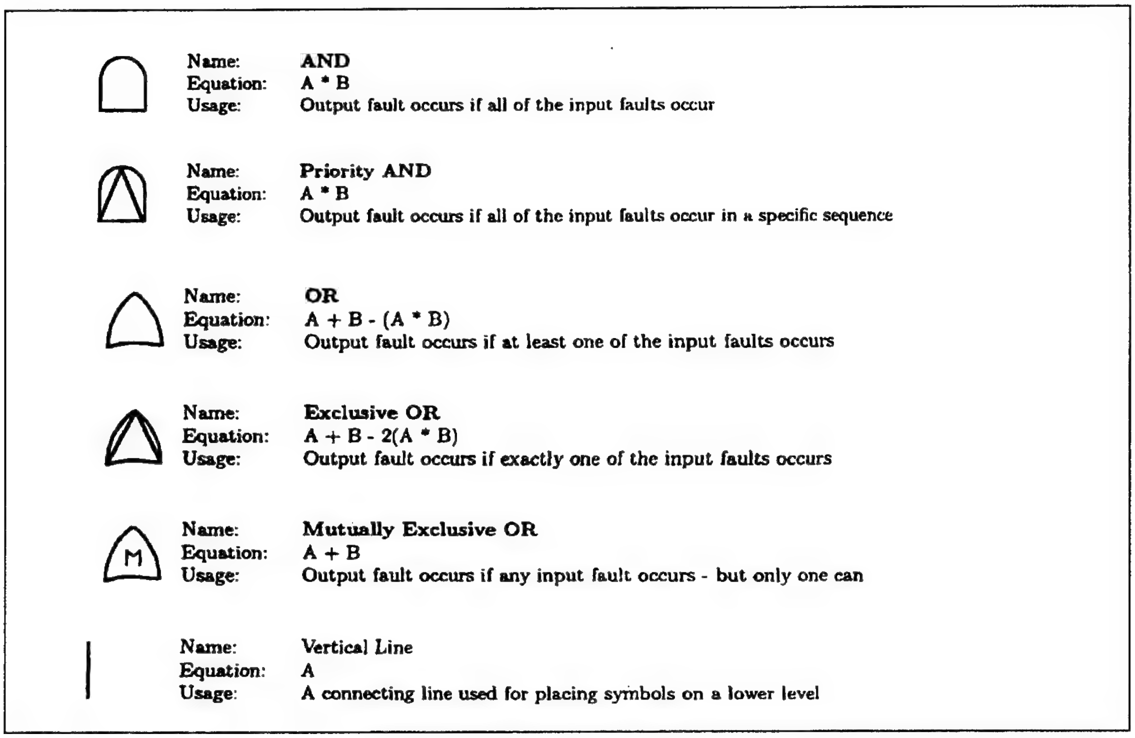
Name: Conditioning Event
Usage: Applies specific conditions or restrictions

Name: Transfer In
Usage: Indicates that the tree is developed further

Name: Basic Event
Usage: A basic initiating fault requiring no further development

Name: Inhibit
Usage: Output fault occurs if the input fault occurs in the presence of an enabling condition

Figure 15. Fault Tree Event Symbology [Ref. 9]



Name: **AND**
Equation: A * B
Usage: Output fault occurs if all of the input faults occur

Name: **Priority AND**
Equation: A * B
Usage: Output fault occurs if all of the input faults occur in a specific sequence

Name: **OR**
Equation: A + B - (A * B)
Usage: Output fault occurs if at least one of the input faults occurs

Name: **Exclusive OR**
Equation: A + B - 2(A * B)
Usage: Output fault occurs if exactly one of the input faults occurs

Name: **Mutually Exclusive OR**
Equation: A + B
Usage: Output fault occurs if any input fault occurs - but only one can

Name: Vertical Line
Equation: A
Usage: A connecting line used for placing symbols on a lower level

Figure 16. Fault Tree Logical Operator Symbology [Ref. 9]

b. Event Classifications

Although a fault tree can contain normal events, the vast majority of events appearing within the tree are failure events. Any event that propagates the failure event needs to be considered during the fault tree synthesis. When defining events, the analyst should observe the no miracle rule. The no miracle rule states that low probability events that prevent fault flow need not be considered, but low probability events that cause fault flow must be considered.

There are five general classifications that describe the failure events that are logically linked in the fault tree structure. [Ref. 5]

(1) Primary Failure. These are component related failures caused by problems internal to the component. Repair of a primary failure will return the system to operation. However, as with the case of PANSAT, repair of primary failures is not typically possible with deployed spacecraft. This is the principle failure type that will be analyzed.

(2) Secondary Failure. This is a component related failure caused external to the component. Repairing a secondary failure does not bring the system back to a functioning condition if the external problems are not additionally addressed. Examples of secondary failures are environmental stresses such as temperature or vibration stress.

(3) Primary Fault. These are event occurrences that create fault flow that are not component related. This could be a normal event or one that is caused by human interaction. A primary fault may self repair.

(4) Secondary Fault. This type of event propagates the fault flow that is externally influenced. If the conditions causing the fault, such as signal jamming, are removed the secondary fault may self repair.

(5) Command Fault. This is defined as a fault or failure which is caused by commands external to the source of the fault. An example would be the inadvertent activation of a relay due to a command fault.

2. Fault Tree Synthesis

The synthesis (construction) of a fault tree should follow a few well-tested rules to avoid logic errors or omission of failure events [Ref. 5]. Definition of the correct top event, that event that is most undesirable, must be accurately considered. The entire synthesis of the fault tree stems from this definition. Accurate boundary conditions are required to predict the various failure events for which that phased mission operating conditions are valid.

The next level is defined below the top event by analyzing what set of events are the most immediate and necessary to cause the top event. At this level, event definition may be very general in nature. To generate the causal events of the preceding event the analysts should ask two general rules. [Ref. 5]

1. What are the most immediate and sufficient causes of this event?

2. Is this a component related event?

Each event is analyzed as to the causation. If the event is caused by a component related event, then an OR gate is placed under the event. If it is not a component related event but a system state related event, then the analyst is free to place any type of gate under the event as deemed logically appropriate. This process is continued, building a logic tree from the top event down to system defined end state events.

E. FAULT TREE EXAMPLE

An example of a simple system is provide to show how fault tree synthesis and analysis is conducted. A comparison of doing the analysis by hand and the analysis generated by the FaultREASE program used is provided.

Consider the simple coherent system depicted in Fig. 17. If component one was to fail, or both components' two and three were to fail, the system would become inoperable. Therefore the minimum cut sets are $\{1\}$ and $\{2, 3\}$. Conversely if components' one and two, or components' one and three were operating then the system would function. This describes the minimum path sets as $\{1, 2\}$ and $\{1, 3\}$. The system structure can be represented using minimum cut set or minimum path set notation. Either approach will give identical results as will be shown below.

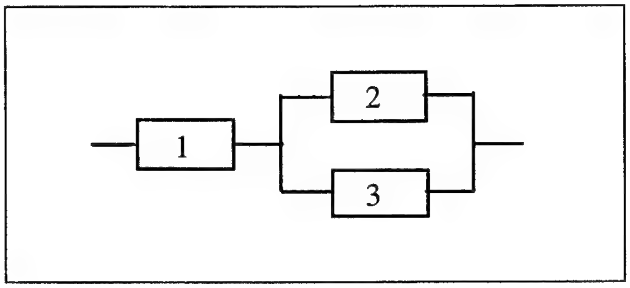


Figure 17. Simple System Functional Structure

1. Cut set notation

It is convenient to represent the system, regardless of the approach, as a graphical representation to aid in further analysis. As the system gets larger and increasingly complex this can become too burdensome. Figure 18 depicts the cut set representation of the system structure.

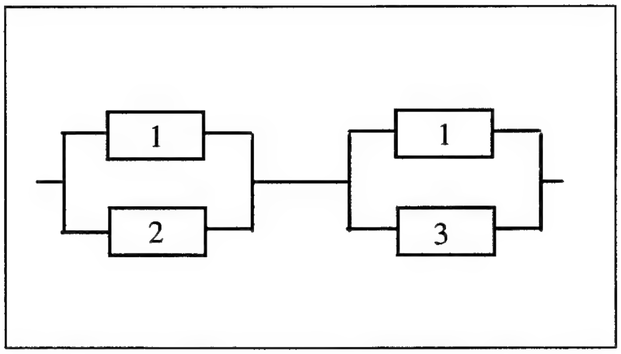


Figure 18. Minimum Cut Set Representation

The minimum cut set functions are derived using eqn 10.

$$\kappa_1(\mathbf{x}) = x_1$$

$$\kappa_2 = x_2 \coprod x_3 = 1-(1-x_2)(1-x_3)$$

From the minimum cut sets, the structure function is determined using eq. 11.

$$\Phi(\mathbf{x}) = \Phi(x_1, x_2, x_3) = \prod_{j=1}^{2} \kappa_j(\mathbf{x})$$
$$= \kappa_1\kappa_2 = [x_1][1-(1-x_2)(1-x_3)]$$
$$= [x_1][x_2+x_3-x_3x_2]$$
$$=x_1x_2+x_1x_3-x_1x_2x_3$$

If the system is assumed to be independent, the reliability function can be derived utilizing eq. 16.

$$h(\mathbf{p}) = E[\Phi(\mathbf{x})] = p_1p_2 + p_1p_3 - p_1p_2p_3$$

2. Path set notation

Similar to the cut set example, the minimum path set graphical representation of the system structure shown in Fig. 19 can be useful.

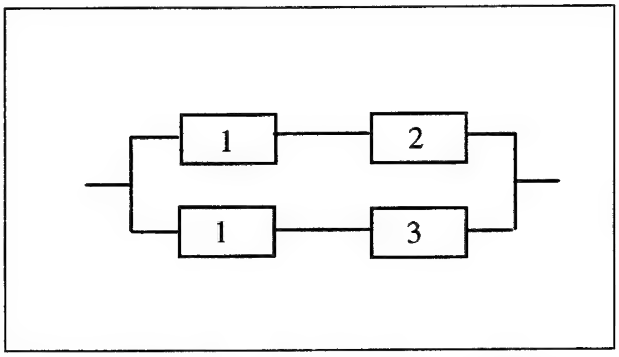


Figure 19. Minimum Path Set Representation

The minimum path sets are derived using eq. 7.

$$\rho_1 = x_1x_2$$
$$\rho_2 = x_1x_3$$

From the minimum path sets, the structure function is determined using eq. 8.

$$\Phi(\mathbf{x}) = \Phi(x_1, x_2, x_3) = \coprod_{j=1}^{2} \rho_j$$
$$= [x_1x_2 \coprod x_1x_3]$$
$$= [1-(1-x_1x_2)(1-x_1x_3)]$$

$$=x_1x_2+x_1x_3-x_1^2x_2x_3 \qquad \text{(recall } x_i^p = x_i\text{)}$$
$$= x_1x_2 + x_1x_3 - x_1x_2x_3$$

As previously stated the path analysis derivation of the structure function is identical to that of cut set derivation. The approach the analyst takes, either cut set or path set, is determined by the type of analysis that is being conducted.

The structural importance of a component in a system is determined by evaluating the state vector **x** under all conditions, while the reliability importance could be evaluated by assigning component reliability values. Assuming component independence the reliability importance can be derived from the reliability function as shown below.

$$I_h(i) = h(1_i, \mathbf{p}) - h(0_i, \mathbf{p}) = \frac{\partial h(\mathbf{p})}{\partial p_i} \text{ (if independent)}$$

$$I_h(1) = p_2+p_3-p_2p_3$$

$$I_h(2) = p_1-p_1p_3$$

$$I_h(3) = p_1-p_1p_2$$

3. Fault Tree Model

The system functional block diagram (Fig. 17) is used to synthesis the fault tree shown in Fig. 20. This was accomplished using the rule set explained previously and incorporating the FaultREASE software package. As an example of the software's computational capabilities, probability values that the components would fail (q_i= 1-p_i) were assigned to the components. The reliability values are represented on the programs printout below the end event leaves.

To illustrate this example, assume the components are independent and have the reliability values of:

$$p_1= 0.9 \text{ and } p_2= p_3= 0.7$$
$$\text{thus } q_1= 1- 0.9 = 0.1$$
$$q_2= q_3= 1- 0.7 = 0.3$$

Using the reliability function derived previously, the system operation reliability can be calculated as:

$$h(\mathbf{p}) = (0.9)(0.7) + (0.7)(0.7) - (0.9)(0.7)(0.7) = 0.819$$

The fault tree, when quantified, will calculate the probability of the top event occurrence (i.e., system failure) to be 0.181, which is shown in Fig. 20 as the value the top event attains. The probability that the system will fail, which is 1-P[system functions], correlates to the probability of success of the system calculated using the reliability function.

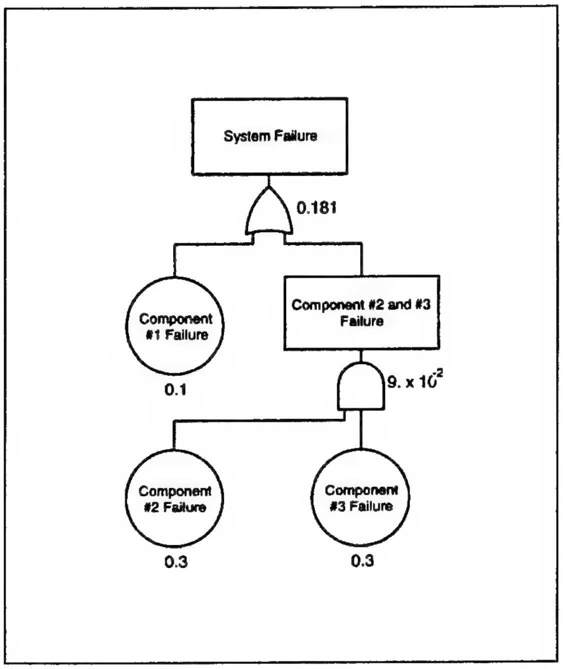


Figure 20. Example System Fault Tree

Table 1 summarizes the calculation of the structural importance for each of the system components. The structural importance of component one is much greater than that of components' two and three that are identical. This intuitively makes sense because component one is a series component and so the failure of this component has a much greater affect on the systems operation.

The reliability importance for each component is calculated and summarized in Table 1. Component one has a higher reliability value, and this coupled with its structural placement demonstrates it's relative effect on reliability importance. By conducting sensitivity analysis on the reliability value for component one it can be shown to retain a higher relative reliability importance than components' two or three.

State Vector	$\Phi(\mathbf{x})$	Component #1	Component #2	Component #3
(0, 0, 0)	0			
(1, 0, 0)	0			
(0, 1, 0)	0			
(0, 0, 1)	0			
(1, 1, 0)	1	1	1	
(1, 0, 1)	1	1		
(0, 1, 1)	0			
(1, 1, 1)	1	1		1
$n_\Phi(i)$		3	1	1
$I_\Phi(i)$		3/4	1/4	1/4
$I_h(i)$		0.91	0.07	0.07

Table 1. Example System Importance

IV. PANSAT FAULT TREE ANALYSIS

The PANSAT schematic diagrams listed as figures in appendices A, B, and C were used to construct the PANSAT fault tree listed in appendix D. Interaction with the specific subsystem design engineers was necessary to ensure interpretation accuracy of the design architecture.

It was never the intention of the author to completely model the design down to the individual component level. From a qualitative analysis viewpoint for the PANSAT project, determination of significant failure points was the overall goal of this thesis. This permits design engineers to assess the fault tree analytical results and make appropriate design modifications as deemed appropriate. The hardware architecture analyzed included the EPS, DCS, and RF subsystems. Time limitations prevented detailed analysis of each subsystem. The majority of the analytical effort was spent on the evaluation of the EPS.

Subsystem design modifications are a natural and continuous process at this stage of the program life-cycle. Modifications made during the course of this analytical process may not be reflected in this analysis.

A PANSAT system structure function could be generated using the minimum cut sets listed in Tables A.2, B.2, and C.2. From the structure function the structural importance of each failure event could be determined by evaluating the function using a system state vector, **x**, of 324 variables correlating to the failure events. Evaluation of the structural importance using the procedure discussed in chapter 3 for this analysis would provide no significant benefit to the design process and be nothing more than an arduous academic exercise. The version of the FaultrEASE software package used for the fault tree construction and analysis did not include the capability for evaluation of the structural importance, although the reliability importance could be calculated if reliability data was available.

A. EPS

The analytical printout of the data derived from the fault tree for the EPS is contained in appendix A. The failure events for the EPS are listed in Table A.1 with a brief description of the component function or failure effect. The event number correlates to the event number listed in the fault tree.

1. Minimum Cut Sets

There are 125 minimum cut sets listed in Table A.2 for the EPS. The number of cut sets is not necessarily a significant measure of a systems architectural resistance to failure. The level of detail for which the analysis is conducted is directly proportional to the size of the analysis elements derived from the architecture. Table A.1 list the failure events or components that were considered to be relevant to the study objective. Many EPS circuits could have been analyzed to increasing detail which would have increased the quantity and size of minimum cut sets. For example, during an iteration of constructing a fault tree for the EPS, a fault tree was constructed which analyzed the electronic power switches in the EPS down to each discrete component level. This sizable fault tree produced over 850 minimum cut sets. Although further detailed analysis could have been conducted on the fault tree, listing many failure points, the effective analysis is no different for the designer than just considering a single end event failure (e.g., switch component failure) for a particular switch. There are many similar examples in the design architecture. The appropriate reduction of the fault tree allowed the analyst to reduce the minimum cut set generation to a more reasonable and analytically more germane size. The largest minimum cut set for the EPS portion of the fault tree consisted of four failure events.

The current version of the FaultrEASE FTA software program is rather elementary in it's capability to model all conditions. The program did not possess the ability to analyze a k-out-of-n structure condition. The single point failure minimum cut sets for the solar panels (i.e., Table A.2 minimum cut sets 1-5) only consider a single solar panel. Since the number of solar panel failures that would be required in order to cause a critical failure is some unknown number k, these failure events would not in reality be single point failures as shown in Table A.2, but would constitute a minimum cut set of size k or greater.

The failure events are listed only once in Table A.1 for convenience, but the actual analysis printout lists the event each time it is repeated. Table 2 lists events in the fault tree that are repeated a number times at various locations within the tree. The number of times the event is referenced could also be an indication of the relative importance of the failure events occurrence. Events 1.134 through 1.135 for example refer to failure events that could cause a failure of the +5 volt power supply. As will be discussed later, this power supply is a very important circuit in the EPS architecture. All other failure events were listed only once.

References to failure events for the remainder of this section refer to the numbers used in Table A.1 and correlate to the respective event numbers on the fault tree. All references to minimum cut set numbers are those used in Table A.2.

Event	#	Event	#	Event	#	Event	#
1.16	3	1.24	6	1.131	15	1.135	15
1.17	3	1.25	6	1.132	15	1.136	15
1.18	3	1.26	6	1.133	15	1.137	15
1.19	3	1.130	15	1.134	15	1.250	2

Table 2. EPS Multiple Failure Event Listings

2. Single Point Failures

Single point failure events are the most significant failure event sets when analyzing the system design for structural reliability. A minimum cut set of size 1 constitutes a single point failure since only that failure event is require to cause the Top Event. The following single point failures are significant to the EPS architecture.

a. +5 Volt Power Supply

The +5 volt power supply is one of the most crucial circuits in the EPS design architecture. This circuit provides power for the majority of logic and control circuits on the spacecraft, including those within the EPS. A parallel redundant power supply is integrated into the circuit design in a warm standby configuration, to instantaneously assume the load in the event of a power supply failure. The current design circuit however does suffer from the possibility of incurring a failure scenario which the failure of one power supply could cause the failure of the second power supply. This is referred to as a contingency redundancy failure and is listed as event 1.110. The two parallel power supplies are connected at the emitters of the power supply output bipolar junction transistor (BJT) from each power supply chip. The collector for each BJT is connected to the raw power bus via a fuse and common input filter. An emitter to collector short for either BJT coupled with the failure of the power supply input fuse to blow for such occurrence (separate fuse for each power supply) would place raw bus power on the +5 volt bus. The consequences of such an occurrence are several, but all result in the failure of the logic circuits to operate correctly.

Table 2 lists failure events relating to a +5 volt power supply failure to be repeated 15 times in the fault tree structure. Failure events for a +5 volt power supply failure are listed as minimum cut sets 11 through 17.

b. Peripheral Control Bus (PCB)

The PCB is a system circuit which is critical for the operation of each of the hardware subsystems analyzed. Responsible for distribution of power, control signals, and data traffic throughout the spacecraft, it has the capability to become a reliability weak link in the system design. With no circuit redundancy for the PCB, almost any single component failure of the circuit could negate the operation and function of every relevant circuit in the spacecraft. The PCB circuit consists of a bus (wire bundle) connecting each subsystem or peripheral component (Fig. A.9), each of which contain interface circuits for power distribution and data connectivity. Failure events for the PCB are listed as minimum cut sets 19-21 and 32-35.

c. Solar Panels

Eight of the 17 solar panels are used for the solar panel illumination experiment (SPIE). Each of these solar panels connect to their individual current sensor (minimum cut set number 1). There are several possible current sensor component failures which could fail in a mode which prevent passing current from the SPIE solar panel to the raw power bus. All 17 solar panels are connected in parallel to supply the raw power bus through the common master current sensor (minimum cut set number 31). The master current sensor is identical to the SPIE current sensors.

It has not been determined exactly how many solar panel failures are necessary to prevent operations as previously discussed. The tumbling motion of the spacecraft complicates the determination of effective solar panel operation or failure. Computer simulations have been written to resemble spacecraft motion and the effective solar flux area [Ref. 10]. The initial failure simulations have been completed analyzing for solar panel failure combinations of size 1 or 2 failed solar panels with the results summarized in Table 3. The effective solar flux area listed is the lowest minimum average for the failed panel orientation to the sun. The power calculations are based upon a 17.1 Watt power budget and effective solar flux area of 989 cm^2.

Solar Panel Failure Size	Effective Solar Flux Area (cm^2)	Percent Power Decrease (%)	Effective EOL Generation (Watts)	Power Decrease (Watts)
1	908	8.2	15.7	1.4
2	831	15.98	14.37	2.7

Table 3. Solar Panel Failure Effects

Each solar panel has a single blocking diode (minimum cut sets 2 and 4) on the connection from the solar panel to the EPS power board. An open diode would prevent power distribution from the solar panel to the raw power bus. A solar panel consist of 32 series connected solar cells. If the panel string integrity is broken (i.e., inter-cell connections or a cell failure), the entire solar panel is rendered useless (minimum cut sets 3 and 5).

d. Control Signals

The operation and commanding of the electronic power switches used in the EPS to distribute the unregulated raw power to the various subsystems is a crucial part of the EPS design. The command signal contains two parts, the switch address and command orders to turn the switch on or off. There are two issues to examine when analyzing how a valid command from the DCS could be misinterpreted at the destination address. These issues are command addressing and command signal errors. The command addressing issue consider how a valid signal address from the DCS is mis-routed or modified in-routed to the destination. The most likely cause of this type of error might be the PCB interface address registers, U17 or U18 on the EPS logic board or a failure of the command signaling path from the PCB interface registers to the switches. The command signaling issue concerns the signal distortion or modification due to a transient condition or circuit malfunction. A recovery from a transient condition may be possible, but a malfunction which places the system in a posture in which ground station intervention is not possible would cause a critical failure. For example a circuit malfunction which cause power to be secured to the RF system when the DCS expected something entirely different like a battery placed on service, would leave the system orbiting without the ability to receive ground instructions. This problem is further complicated by the inability of the DCS to determine if the signal it has commanded has been accomplished as ordered. The DCS only has the capability to command switches, and has no way to directly read the position of the switch (i.e., on or off). Failure events for the control issues are lists as minimum cut sets 36 and 37.

e. EPS Logic Board

The EPS logic board can be thought of as the workhorse of the EPS. The logic board conducts the commands received from the DCS for power switching, power measurements, and WDT resets. Single point failures of the logic board pertain to the ability to route the correct DCS commands and WDT reset signals. Minimum cut sets 21, 25, 26, and 38-46 will prevent command signals from reaching their destination. The WDT and the circuits used to reset it are listed as minimum cut sets 18, 21-30, 32, 40, 43, and 46. The logic board is designed almost exclusively using integrated chips (IC) with very few discrete components. Analyzing the logic board to the component level (i.e., IC level) there is virtually no component which is not a single point failure. The high threshold detector failure (failed high) would prevent any reset command from resetting the WDT. The purpose of the high threshold detector is to prevent the cyclic resetting of the WDT when there is a low voltage condition on the +5 volt power bus until the bus becomes stable. The most likely time this would come into play is during spacecraft initialization. The low threshold detector (fail low) would maintain logic components U21, U22, U25, U26, and U27 in a initialization condition (i.e., unable to apply power to mass storage, TMUX, RF, antenna release circuit, or battery switch operations). Any failure which causes the output of U27 (D flip-flop which signals for power application to a DCS) to fail high or low could cause the system to fail.

f. Thermal Control

Since the system is designed without an active thermal control system, all temperature sensitive components must rely on accurate thermal analysis. Accurate reliability prediction also requires a well defined thermal environment prediction. A failure of the passive thermal control system to maintain the spacecraft within it's operational boundary limits or the failure of swift ground station operator action to a unusual thermal condition can lead to component failures throughout the design structure. The battery compartment is sensitive to excessive thermal conditions. If the temperature of the battery compartment exceeds the thermal limits, then battery cell plate degradation and shortened battery life should be expected. Temperature conditions which exceed the thermal limits could cause cell dryout due to excessive cell pressure compromising battery seal integrity. Single point failures due to improper thermal control are listed as minimum cut sets 6, 7, and 8.

g. Battery Monitor

The battery monitor is responsible for maintaining an accurate estimation of the condition of the on-board batteries. A failure of the monitor to maintain a precise prediction could cause the operation of a battery outside its preferred operating envelope. This could lead to a shortened battery lifetime. A failure of the battery cell voltage and current sensing circuits could cause the battery monitor to make incorrect estimations. If the respective sensors, addressing registers, or multiplexers were to fail the battery monitor would receive inaccurate data. This is listed as minimum cut sets 9 and 10.

3. Double Point Failures

As the minimum cut set size increases, the systems reliability structural also becomes more favorable. There are three EPS circuits which exhibit minimum cut sets of event size two. These are the launch switches, WDT, and storage batteries.

a. Launch Switches

The launch switches, as presently designed, are configured in two parallel strings of two series connected switches (Fig. A.1). Such a design generates a minimum cut set list that consist of failure combinations of one switch from each parallel leg (minimum cut sets 47-50). The four minimum cut set combinations are listed as minimum cut sets 47-50.

b. Battery

The two parallel storage batteries generate a list of double point failures. Each battery consist of a number of single point failures, but when the battery system is considered as a combination of both batteries a double point failure circuit is generated. Battery testing is currently in progress to determine battery operating characteristics. The failure events listed for the batteries are failure event types common to Ni-Cd batteries. Minimum cut sets 47-99 list the battery double point failures.

c. WDT

The most critical portion of the WDT is the D flip-flop which switches power to the respective DCS. As previously discussed as a single point failure, if U27:A fails then the system fails. This single point failure can also be described as a double point failure in which both outputs (Q and Q bar) fail to a low condition. This is listed as minimum cut set 105. It is also possible for U27:A to fail in a condition in which both outputs fail to a high condition (minimum cut set 104). If this condition exists, then power is continuously applied to both DCS A and DCS B. The respective DCS have no means to communicate with each other. If one DCS is operating it assumes it is the only DCS that is functioning. This can cause fatal operational control of the spacecraft, with the respective DCS's fighting over the systems operations. Scenarios could be easily conceived in which the system places itself into a unrecoverable state by one DCS placing the system in a given state and the other DCS, assuming a different initial conditions, altering the system state to an unrecoverable condition. For example, assume DCS A has the system aligned in the following conditions listed in Table 4.

Then a failure to U27:A occurs and power is additionally applied to DCS B which initializes the spacecraft and DCS B re-configures the spacecraft into the listened mode described in Table 5 without the detection of DCS A.

DCS A will remain in a listening mode, but will never receive a signal due to the fact the configuration has been modified to send the signal to DCS B. DCS B is in a listening mode waiting for NPS connection and operating system upload. When DCS A does not receive a signal after a given period of time it will modify it's assumed configuration, say switch over to LNA #2, which secures power to LNA #1, applies power to LNA #2, and switches RF S2 and RF S4 to LNA #2. Now no signal will be received by DCS B, for which it will modify the system configuration. This cycle could continue indefinitely.

EPS	DCS A	RF
Batt. A on-line switch closed	DCS A receive segment lined up to RF	Power applied to LNA #1 circuit
RF power switch on		RF S1 selected to receive
TMUX A/TMUX B power switch closed		RF S2 selected to LNA #1
Ant. Deployment 1 and 2 power switches open		RF S4 selected to receive from LNA #1
MASS A and B power switches closed		RF S5 selected to receive mixer
All battery charge and discharge switches open		RF S6 selected to receive mixer
WDT U27:A output to DCS A		RF S7 selected to receive
		RF S8 selected to DCS A receive

Table 4. DCS A System Configuration

EPS	DCS B	RF
Battery A on-line switch closed	DCS B receive segment lined up to RF	Power applied to LNA #1 circuit
RF power switch on		RF S1 selected to receive
TMUX A and TMUX B power switch closed		RF S2 selected to LNA #1
Ant. Deployment 1 and 2 power switches open		RF S4 selected to receive from LNA #1
MASS A and B power switches closed		RF S5 selected to receive mixer
All battery charge and discharge switches open		RF S6 selected to receive mixer
WDT U27:A output to DCS B		RF S7 selected to receive
		RF S8 selected to DCS B receive

Table 5. DCS B System Configuration

Another critical system operation could occur in the mass storage devices with the competing DCS microprocessors' overwriting essential data used for the other microprocessor specific computations.

4. Triple Point Failures

a. Solar Panels

The structural reliability of the solar panels have been increased by adding a second line from the solar panels to the EPS power bus, both for the line and return lines. There are fuses at each end of the power lines to prevent a fault (i.e., power line to ground short) from grounding out the solar panel and/or the raw power bus. This design generates the minimum cut sets 103-110. There in actuality would be 8 minimum cut sets for each solar panel, but only one solar panel was included in the fault tree due to software limitations.

b. Battery

Blocking diodes on the output of each battery prevent uncontrolled battery charging. If the diodes were to open then no current could flow from the battery to the raw power bus. Increased structural reliability was accomplished by placing two diodes in parallel on the output of each battery. Minimum cut sets of size 3 are therefore found by having both diodes of one battery fail concurrent with a critical failure in the other battery. These are listed as minimum cut sets 111-124.

5. Quadruple Point Failures

a. Battery

As discussed above, both batteries have two blocking diodes in parallel on their output. Therefore one possible failure scenario is if all four diodes were to fail open. This is minimum cut set 125.

6. Improvements

During the process of synthesizing the fault tree for the EPS several design modifications have been made which have increased the subsystem reliability. These issues, along with some further suggestions, are discussed here to provoke further thought in design enhancement considerations.

a. Launch Switches

The PANSAT design exceeds the safety requirement mandated by NASA with the use of the parallel launch switch design (Fig. A.1) for launch from the space shuttle. The NASA requirement stipulates two series connected switches to prevent powering up the system and possible radiation of electro-magnetic energy from the satellites communication subsystem while still in the shuttle cargo bay. The parallel switch design effectively doubles the reliability of the launch switch circuit. Further analysis has revealed that the circuit reliability can be further strengthened at no cost or major design modifications. Figure 21 illustrates the modification of the present design by placing a single wire between the junctions of the series connected switches. The NASA requirement of two switches connected in series from the power source to the load is still satisfied.

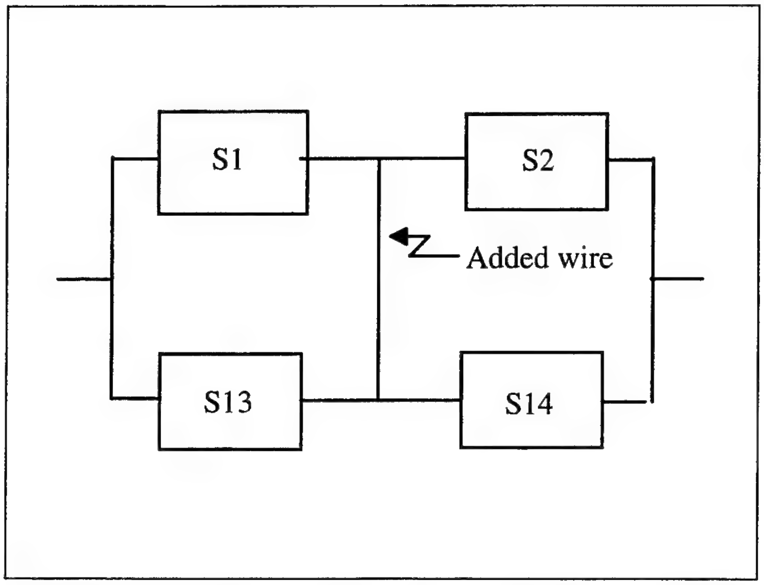


Figure 21. Alternate Launch Switch Configuration

The current design results in four minimum cut sets of size two failure events. The alternate configuration (Fig. 21) results in a much more stringent launch switch configuration design. The minimum cut sets for the alternate design are listed in Table 6. The event type "circle" refers to a basic component failure, in this case it is the launch switch failure in the open position.

The system structure functions for the launch switch circuits can be derived using equations 10 and 11 to the current and alternate launch switch configurations shown below. If the switches are assumed to be independent and identical then the reliability function can also be derived. Functions with a subscript of the letter C are a reflection of the current launch switch design configuration, and those subscripted by the letter A relate to the alternate configuration. Derivation of the following results are similar to the example problems provided in Chapter III.

(1) Current Configuration

$$\kappa_1 = s_1 \coprod s_{13};\ \kappa_2 = s_1 \coprod s_{14};\ \kappa_3 = s_2 \coprod s_{13};\ \kappa_4 = s_2 \coprod s_{14}$$

$$\Phi_c(\mathbf{s}) = \prod_{i=1}^{4} \kappa_i = s_1 s_2 + s_{13} s_{14} - s_1 s_2 s_{13} s_{14}$$

$$h_c(\mathbf{p}) = p_1 p_2 + p_{13} p_{14} - p_1 p_2 p_{13} p_{14} = 2p^2 - p^4$$

$$I_{h_c}(i) = \frac{\partial h_c(\mathbf{p})}{\partial p_i} = p - p^3 \text{ (Since all switches are assumed identical)}$$

(2) Alternate Configuration

$$\kappa_1 = s_1 \coprod s_{13};\ \kappa_2 = s_2 \coprod s_{14}$$

$$\Phi_A(\mathbf{s}) = s_1 s_2 + s_1 s_{14} + s_2 s_{13} + s_{13} s_{14} - s_1 s_2 s_{13} - s_1 s_2 s_{14} - s_1 s_{13} s_{14} - s_2 s_{13} s_{14} + s_1 s_2 s_{13} s_{1}$$

$$h_A(\mathbf{p}) = 4p^2 - 4p^3 + p^4$$

$$I_{h_A}(i) = 2p - 3p^2 + p^3$$

If the alternate configuration is more reliable, then the reliability function for the alternate configuration must be greater than the reliability function for the current configuration for all reliability values, p, of the launch switch (each switch is assumed identical).

Hypothesis:

$$h_A(\mathbf{p}) \geq h_C(\mathbf{p})$$

Proof:

$$h_A(\mathbf{p}) = 4p^2 - 4p^3 + p^4 \geq 2p^2 - p^4 = h_C(\mathbf{p})$$

$$2p^2 - 4p^3 + 2p^4 \geq 0$$

$$2p^2(p^2 - 2p + 1) \geq 0$$

$$2p^2(p - 1)^2 \geq 0 \quad \text{for all } 0 \leq p \leq 1$$

Min Cut Set	Min Cut Set Size	Event Type	Description
1	2 events	CIRCLE	S2 Failure
		CIRCLE	S14 Failed
2	2 events	CIRCLE	S1 Failure
		CIRCLE	S13 Failed
3	3 events	CIRCLE	S13 Failure
		CIRCLE	S1 Failure
		CIRCLE	S14 Failed
4	3 events	CIRCLE	S13 Failure
		CIRCLE	S1 Failure
		CIRCLE	S2 Failed
5	3 events	CIRCLE	S14 Failure
		CIRCLE	S2 Failure
		CIRCLE	S1 Failed
6	3 events	CIRCLE	S14 Failure
		CIRCLE	S2 Failure
		CIRCLE	S13 Failed

Table 6. Alternative Launch Switch Configuration Minimum Cut Sets

Therefore the alternate configuration is more reliable at the cost of a small wire connecting the switches. The ratio of the reliability functions will give a good indication of the relative value of the alternate configuration. As the individual switch reliability (p) approaches one, the ratio also approaches one.

$$\frac{h_A(\mathbf{p})}{h_C(\mathbf{p})} = \frac{4p^2 - 4p^3 + p^4}{2p^2 - 4p^4} = \frac{(p-2)^2}{2-p^2}$$

b. Blocking Diodes

(1) Battery Blocking Diodes. A preceding EPS design used one output blocking diode from each battery to the raw power bus. Using an approach similar to the above, it can be shown the reliability for the blocking diode circuit increases from a value of p to a value of $2p\text{-}p^2$. This will increase the reliability of the diode circuit for all reliability values p.

(2) Solar Panel Blocking Diodes. The approach to dual blocking diodes used for the battery can also be applied to the solar panel and elsewhere in the EPS design where appropriate space availability exist. This is a critical component for the solar panels and could be incorporated into the design at a relatively low cost.

c. Power Switching Control Circuits

The power switching logic circuits on the EPS logic board are single point failure items for the system. The distribution of load assignments to the power switching control registers, U21 and U22, are shown in Fig. A.3. All similar type loads are controlled off the same register. The failure of one register would prevent the use of both redundant subsystem circuits. The loads for U21, for example, control all the switches for charging, discharging, and placing on-line both batteries. If U21 were to fail, then no battery switch would be functional, and would cause a critical failure. In order to help reduce the possibility of a single point upset by the failure of one register, like subsystem components should be controlled off separate registers (i.e., MASS A controlled by U21 with MASS B controlled by U22). Additionally, all the switches for a particular battery must be controlled off the same register to prevent a similar type failure scenario with the present design.

Consideration for failure modes which place the spacecraft in a configuration in which two-way communication with the satellite is not possible should be addressed in the operating system architecture. To prevent the spacecraft from re-configuring to a failed alignment, particularly after an upsetting event has caused a system re-initialization, a log of the systems configuration should be maintained within the flash memory of the mass storage devices.

The ability to verify system commands could be beneficial to the satellites self diagnostics capability and a basis for critical failure mode prevention. If the satellite possessed the ability to recognize the systems failure to correctly respond to commands it has ordered, it could re-configure to an acceptable configuration before a critical failure event has occured, and allow further analysis to be conducted by the ground station.

d. Antenna Deployment Circuitry

Detailed failure analysis of the communication signal beam pattern has not been studied for a failure scenario in which a portion or all of the antenna circuits' four dipole antennas fail to release. A second power switch was added to the design to help ensure the deployment of the antennas. The additional switch feeds a common antenna deployment circuit consisting of heaters to burn the antenna restraints. A failure in the antenna deployment circuit would still prevent a controlled antenna release. A deployment circuit with parallel switches connected in this configuration also risks the possibility of a contingency redundancy failure of the switches. True circuit redundancy is only possible if the circuits are independent of each other.

e. Solar Panel Wiring And Fusing

Redundant power lines (both supply and return) from the solar panels to the EPS power board have been added to prevent the break in one line from isolating a solar panel. Additionally, fuses at each end of the supply line are provided to prevent a short from grounding out the panel.

f. Power Switch Fusing

Fuses at the input of each power switch, with the exception of the RF power switch, have been added to prevent a short in a subsystem grounding out the entire spacecraft power bus.

g. +5 Volt Power Supply

The +5 volt power supply performs a crucial role in the performance of the spacecraft. Used for most control circuits, it's failure in any way will cause a critical failure. Minimum cut sets relating to the +5 volt power supply failure was listed conservatively 16 times for the EPS portion of the fault tree alone. Although there is a redundant power supply, the susceptibility of the design to a contingency redundancy failure should not be overlooked. Further analysis, using quantitative analysis, is necessary to validate the power design configuration.

h. PCB

The PCB is the vital communication and power distribution link between the subsystems and peripherals. A single failure (e.g., break in a power line from the EPS) could permanently secure operations. Short of making a redundant PCB, which defeats the compact design of the PCB, only stringent quality control of the PCB fabrication and installation can help minimized the failure of the physical bus. Although the PCB interface circuits are radiation hardened, there is no redundancy provided for any circuit interface.

i. WDT

Any failure condition of the WDT, particularly U1 and U27:A, will result in a critical failure. If the circuit was to fail in a condition in which both DCS A and DCS B are powered, then the system must be intelligent enough to detect and responded in a manner to maintain the system operational. One possible solution is to reserve a given memory location in the mass storage devices for the operational DCS to access. If a DCS is functioning, then it would periodically read that memory location contents for it's unique identification flag. If the memory location did not possess it's flag, but instead contained the flag of the other DCS, as would be the case if both DCS were accessing the location, then it would reset the flag. If the flag had been altered at the time of it's next access, it would then go into a standby condition and allow the other DCS to control the spacecraft. This standby mode, for example, could be the continuous calculation of the value of pi to keep the microprocessor busy. The other DCS must also detect the other DCS status and make that report in the telemetry stream to the ground station.

j. Battery

The battery must be periodically reconditioned using controlled battery discharge and charging procedures. This will increase battery lifetime and also result in resetting the battery monitor to a known condition of battery status.

B. RF

The RF subsystem fault tree was constructed utilizing the block diagram (Fig. B.1). The respective switch designations (i.e., RF S1 through RF S9) are unique to this analysis only. These may not correlate to the designations used by the subsystem designer in future schematics. The RF subsystem is designed with redundant circuits and selective switching circuits to route the signals. This makes the application of the signal routing switches the critical failure points for the design. The reliability of the switching circuits and the control system must be carefully evaluated to ensure the reliability of the system is actually enhanced by the use of similar redundant systems.

The analysis data derived from the fault tree for the RF subsystem is contained in appendix B. The failure events for the RF subsystem are listed in Table B.1 with a brief description of the component function or failure effect. The event numbers correlate to the event number listed on the leaves of the fault tree.

1. Minimum Cut Sets

There are 114 minimum cut sets (Table B.2) for the RF subsystem portion of the fault tree. Minimum cut sets of size 1 (single point failures) contribute to 90 of the 114 minimum cut sets. The majority of the event types are listed as a "diamond" event (Fig. 15), as described in Chapter III. This indicates that further evaluation of the event is possible but is not conducted here. This may be due to the fact no additional information could be derived by further breaking down the design, the immaturity of the design, or due to analysis time limitations.

2. Single Point Failures

The prevalent single point failure events involved the signal routing switches in the RF subsystem, from the antenna to the respective portions of a DCS modem. The other single point failure events consider antenna and power supply failure scenarios.

a. Signal Routing Switches

There are 63 single point failures corresponding to the switch operations alone. There are 7 single point failure events listed for each of the 9 RF signal routing switches. The issues concerning a switch failure include switch component failures, command bus failures, command addressing logic failures, command signal format problems, and power distribution from the respective power buses to the circuits. The failure events for RF switch #3 (Fig. B.1), for example, are listed as minimum cut sets 11-17. Two of the switches, RF S1 and RF S2, are mechanical switches and thus subject to the additional failure mode of mechanical wear. The switch failure events themselves have not been addressed in significant detail due to time constraints.

Since the signal routing switches are common and necessary option for parallel circuit operation with the given design, they could also be listed as a part of a double point failure minimum cut set. This is because the switch failure position can be one of several modes. It could fail in a condition in which it could not route the signal in either direction (i.e., RF S2 could not route signal to LNA #1 or LNA #2), in which it would be a single point failure. The switch could also fail in a condition in which it could only route the signal through one path (i.e., LNA #1) so that an additional critical failure event in the path selected by the failed switch would be required for a critical failure. Additionally, if the switch was common to both the receive and transmit circuits (i.e., RF

S1, RF S4, RF S5, RF S6, or RF S7) then it's failure may diminish the satellite to a given operational function (i.e., transmit or receive). If that were true, then the system would be functionally inoperable, lending itself as a critical failure.

b. Antenna

The critical failure events associated with the antenna circuits, which include the antenna, impedance matching transformers, interconnections, and the bandpass filter, consider the events which diminish the communication signal to noise ratio. Minimum cut sets 32-45, 54, and 55 are concerned with signal grounding, degraded signal path characteristics, and component failures. For the antenna circuit the key to it's successful operation is inherent to quality fabrication and system interface.

c. Power Supply

The RF subsystem electrical power concerns are associated with the distribution of power from the PCB interface for the RF subsystem. Using both power from the +5 volt bus for PCB interface and command signal processing, the local +5 volt bus is as important to the RF subsystem as it was to the EPS.

Raw power from the EPS is locally conditioned (regulated) for use by the RF subsystem components. A critical failure event to the local power buses will cause a system failure.

3. Double Point Failures

There are 24 minimum cut sets consisting of 2 failure events for the RF subsystem. Since there are only a few circuits which constituted the subsystem, and most circuits are redundant, there are only a few double point failures listed for this analysis.

a. Antenna Deployment

The failure of the antenna to properly deploy, whether it be during controlled deployment efforts during the launch and initialization phase or fails to manually deploy following, may be a critical failure mode. Detailed analysis of antenna beam patterns with the dipole antennas housed, or partially deployed, must be conducted to determined if a sufficient signal to noise ratio can be supported. Minimum cut set number 102 list low battery power a causation for the antenna failing to release. This may not actually be a viable cause since battery power is not relied upon as a power source for antenna deployment.

b. Amplifiers

There are two HPA circuits, each consisting of two cascaded power amplifiers. Any two combinations of a amplifier from each HPA will prevent signal transmission. These are listed as minimum cut sets 91-95.

Each of the two LNA's contain one amplifier circuit. This requires both LNA's to fail, or one LNA failure coupled with an associated switch, RF S2 or RF S4, failure.

c. Intermediate Frequency (IF) Circuits

The signal conversion from pass band to IF, or vice versa, takes place in one of two frequency conversion circuits. Each circuit consist of a signal mixer and dedicated local oscillator (LO). The LO can prevent operations by either component failure or significant frequency drift.

4. Improvements

The prevalent concern from a reliability structure of the RF subsystem originates with the signal routing structure. Both component and command signaling concerns dominate the signal path issues. Although it is not easy to expose the true reliability weakness of the design without assigning quantitative values, a more reliable system may be one which consist of only a few necessary switches.

C. DCS

The DCS was the subsystem which received the least attention due to time limitations. The analysis therefore should not in the least be considered detailed or complete. All the data derived for the DCS portion can be found in appendix C. The system failure events, listed in Table C.1, are not at all detailed, considering only very generic failure scenarios. There are 55 minimum cut sets for the DCS and are listed in

Table C.2. A block diagram (Fig. C.1) was used to construct the DCS portion of the fault tree.

Since the fault tree was constructed at a very generic level, the majority of the failure events result in single point failure conditions. There are 54 single point failures listed for the DCS. Each failure event is a circuit malfunction. There is one double point failure and it refers to the peripheral mass storage device failures.

A more thorough analysis of the DCS is required to generate any constructive analysis data which has not yet been already discussed in the previous sections.

V. SUMMARY

Sound system management requires the exploitation of all relevant analytical capabilities to ensure the most reliable system is deployed. Essential to the design architecture of any system is the effort to minimize all system failure modes. The principal theme of this thesis has been to identify the critical failure modes for the PANSAT EPS, DCS, and RF subsystems using fault tree analysis to permit architectural modifications that are essential to meeting the systems operational lifetime requirements.

Continuous maintenance of the fault tree is required if it is to be of continuing benefit in the design process and helpful in explaining the cause of system anomalies during test and flight.

Significant weak points in the design have been identified and should be the topic of further design modifications and analysis. This will require further detailed modeling and assessment efforts.

A. SYSTEM RECOMMENDATIONS

The analytical efforts discussed in chapter 4 indicate the design concerns which should be considered. The most prevalent questions that require attention follow:

1. The +5 volt power supply reliability and its susceptibility to a contingent failure are of great concern. This critical circuit effects each subsystem in a very critical manner. Detailed analysis of the present design, as well as alternative designs should be evaluated to enhance the circuits reliability.

2. The PCB is the artery that supports the entire spacecraft. If it is severed in any manner, then the spacecraft is sure to experience a critical failure.

3. Command switching operations are a necessary function of the system due to the design structure. The EPS and RF subsystems both rely upon intelligent switching operations to complete their mission. The system is not presently capable of making an informed evaluation of its state (i.e., switch positions). Consequently, historical command data must be relied upon to reconfigure the spacecraft for each operation.

4. The EPS logic board consists of circuits with no redundancy. Almost without exception each component could cause a critical failure. Circuits that perform

redundant operations should not be linked, if all possible, through a single point failure. For example, redundant components should not be addressed through the same addressing register for switch control operations.

5. The launch switch circuit, in its present configuration, constitutes a system that has an equivalent minimum cut set representation of size two event elements. Although this is more structurally secure than the single point failure events, it has been proven that at the cost of a short wire the circuit can be made more reliable.

6. The energy storage batteries being flown aboard the spacecraft are not space qualified. It is important for the endurance and survivability of the batteries that they be operated within operational bounds and placed on a stringent maintenance schedule.

7. Detailed evaluation of all switches, both mechanical and electronic, should be carefully studied to determine their respective reliability. For a given system it may be more appropriate to simplify the design and not rely upon sophisticated signal routing.

8. Testing and subsystem integration procedures are important elements to help minimize some of the failure events listed in the fault tree. Assessment of external stresses (i.e., structural and thermal stress) upon the spacecraft, and the order of their occurrence, can have dramatic effect on the system reliability performance. An example of such stress would be thermal expansion that causes broken component leads and connections. Thermal excursions can affect the reliability of components, and must be considered when evaluating the components reliability. Stress screen testing, typically performed by the vendor, of electronic components is an effective tool to minimize electronic circuit component failures.

B. SYSTEM RELIABILITY MANAGEMENT

A severe weak point in the PANSAT program has been its cursory approach to reliability analysis. The absence of a coherent reliability program that supports the design process has resulted in a program with no analytical basis. This would not be permitted in any commercial or defense contractor program.

This thesis has been the lead reliability analysis of the program, and has occurred at a late stage of the systems design lifecycle. There are numerous publications that outline how a reliability program is incorporated into a systems design and operational cycle. Several military standard (MIL-STD) publications are available that deal directly with the programmatic structure a reliability program should embrace. These are briefly discussed to promote further thought by systems management personnel.

1. Reliability Program for Systems and Equipment Development and Production (MIL -STD-785)

This standard provides the general requirements and specific tasks for reliability programs during the development, production, and initial deployment of systems and equipment [Ref. 11]. Designed for use by Department of Defense (DoD) contractors, it provides the guidelines for effectively designing, managing control, and reliability maintenance essential for a reliability program.

2. Reliability Program Requirements for Space and Launch Vehicles (MIL-STD-1543)

This standard is similar to MIL-STD-785 but is tailored specifically for the DoD space systems contractor. Detailed requirements of reliability design reviews, reliability modeling requirements, testing, and corrective action review boards are provided to integrate the reliability and design processes [Ref. 12].

3. Procedures for Performing a Failure Mode, Effects and Criticality Analysis (MIL-STD-1629)

This standard establishes the requirements and procedures to perform a failure mode, effects, and criticality analysis (FMECA). This tool could be used to systematically evaluate and document the potential impact of each functional and hardware failure on mission success, safety, performance, maintainability, and maintenance requirements [Ref. 13]. The use of FMECA is typically used as a management and reliability assessment tool for program design reviews.

C. FOLLOW ON STUDY

The need for reliability analysis assessment has become increasingly evident as the thesis effort has progressed. Several issues that need to be explored for the PANSAT program and any follow on program are listed below:

1. More detailed analysis of specific subsystems and circuits is required. Although a significant amount of analytical information was uncovered, only the ground work has begun on this topic. There is an abundant amount of data that could be investigated to enhance the design process.

2. A detailed reliability management plan should be created and complied with in order to head off problems early in the design cycle. This will help ensure that key reliability issues are addressed right from the programs inception. This goal could expand the realm of the programs involvement to include students and staff from the Operations Research Department (OR), where experience and involvement in similar programs dealing with these types of issues are in progress.

3. As the design reaches maturity, a quantitative analysis modeling of the system could provide useful insights to the missions reliability state.

4. The fault tree constructed for this thesis must be continuously updated and built upon as the design changes and matures. It is strongly recommended that this task be assigned to a program engineer.

APPENDIX A. ELECTRICAL POWER SUBSYSTEM

FAULT TREE ANALYSIS

This appendix contains the raw data for the FTA of the EPS. Figures A.1 through A.9 are EPS schematic diagrams. The EPS failure end events are listed in Table A.1 and Table A.2 lists the EPS minimum cut sets generated by the FaultrEASE fault tree software program for the PANSAT fault tree in Appendix D.

The minimum cut sets were generated using a direct evaluation technique employed by the fault tree software program. The basic end events were compared by their description label contents.

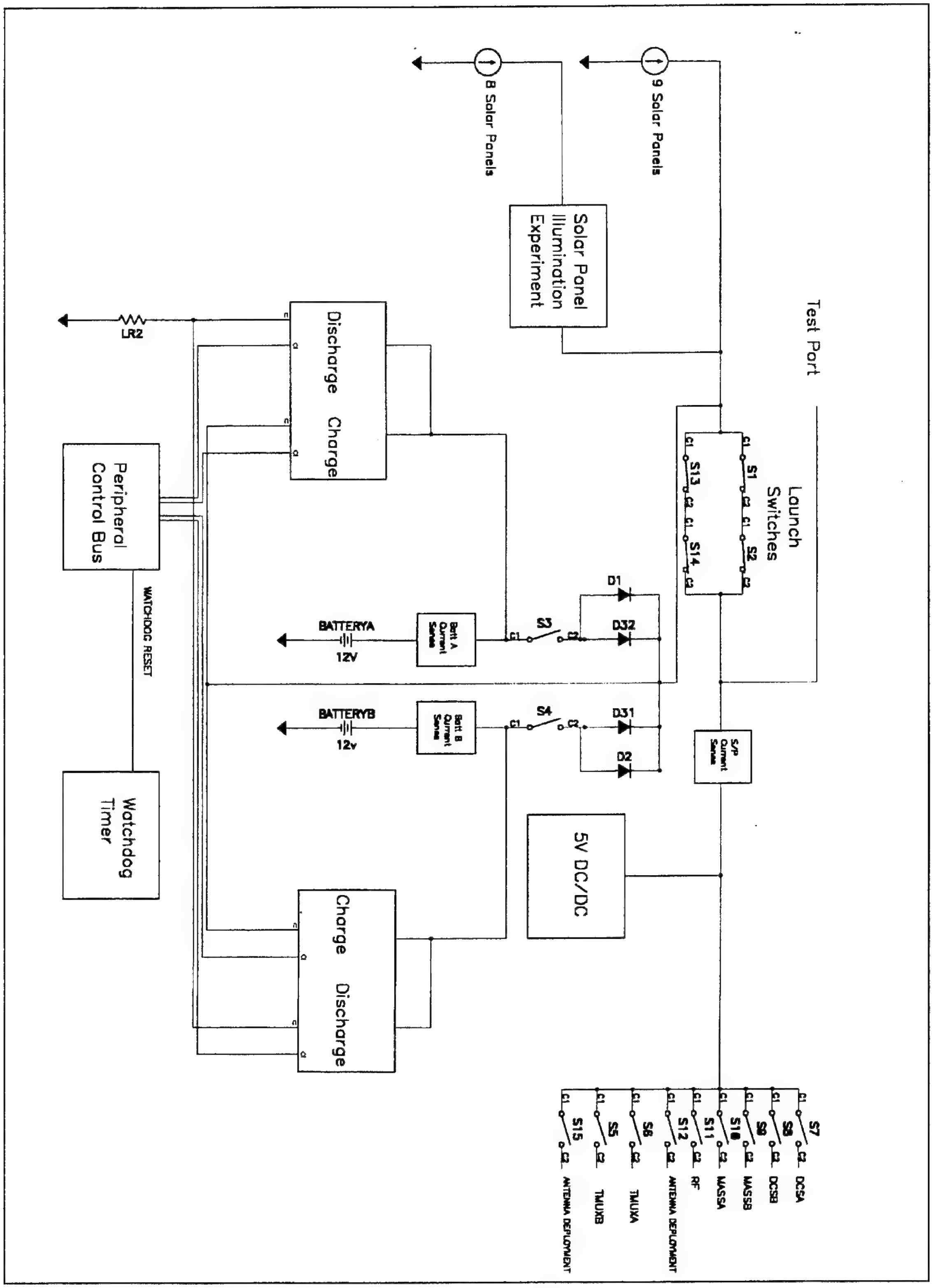


Figure A.1 EPS Block Diagram

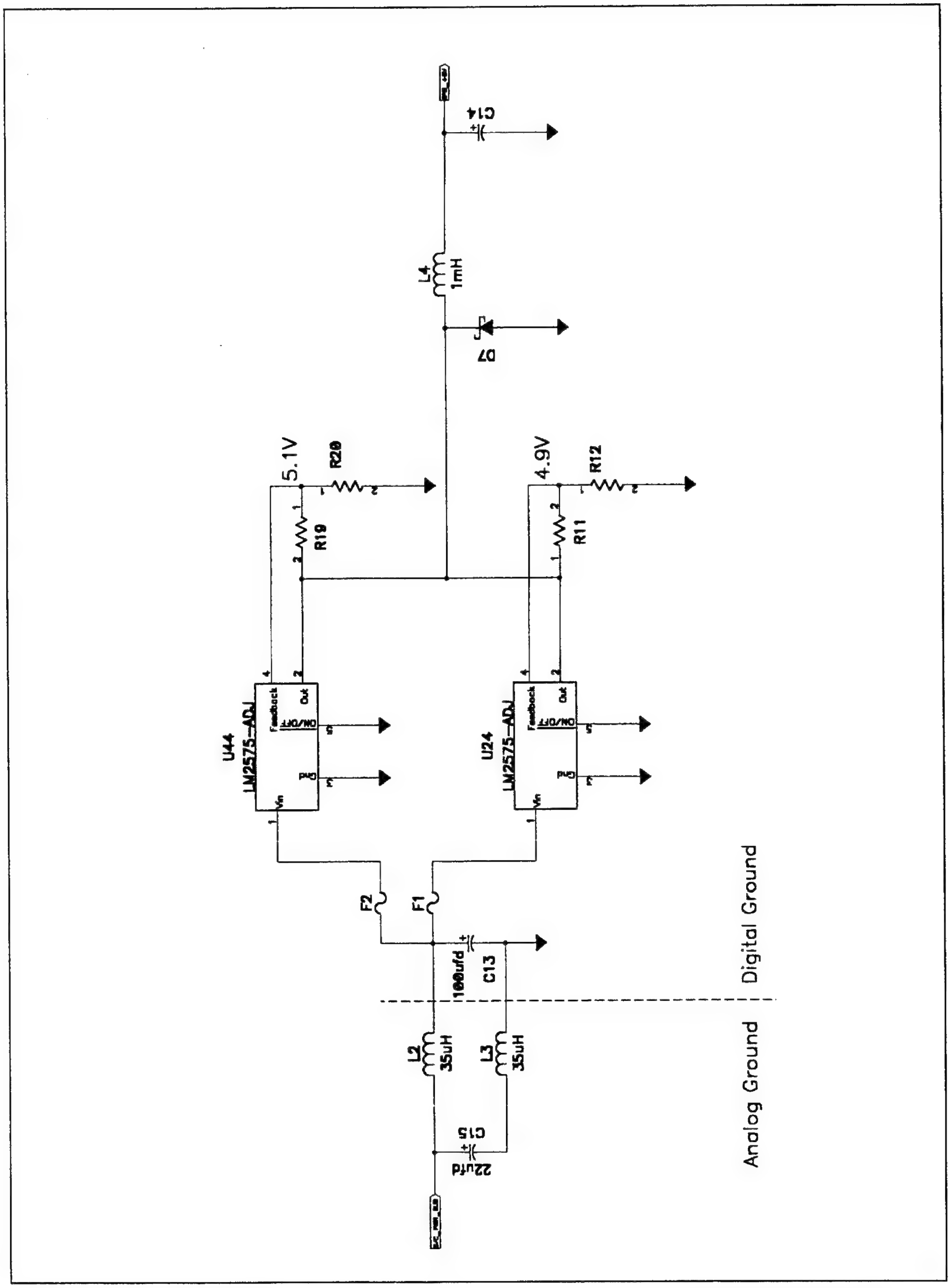


Figure A.2 EPS +5 Volt Power Supplies

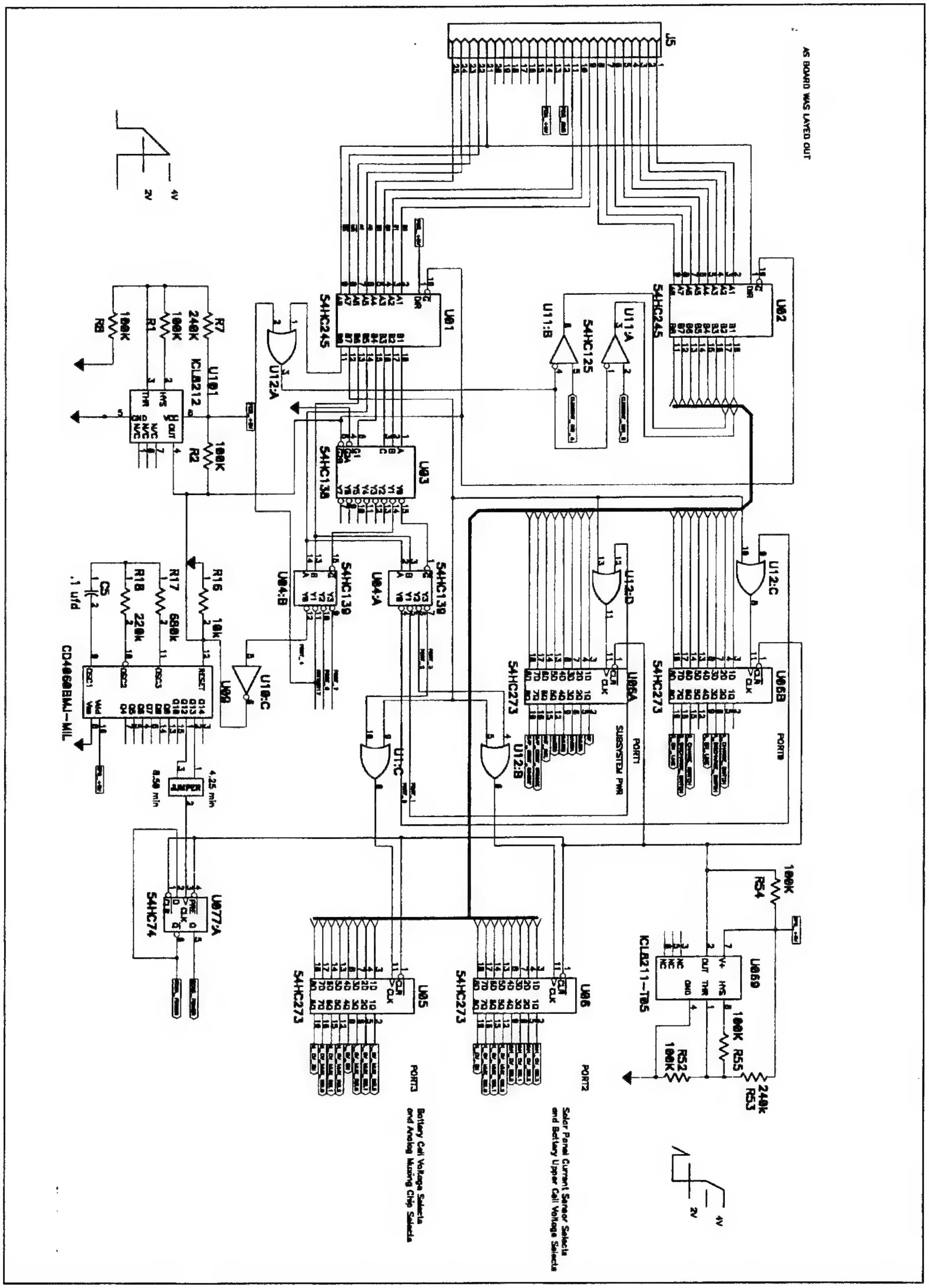


Figure A.3 EPS Logic Circuit and Watchdog Timer

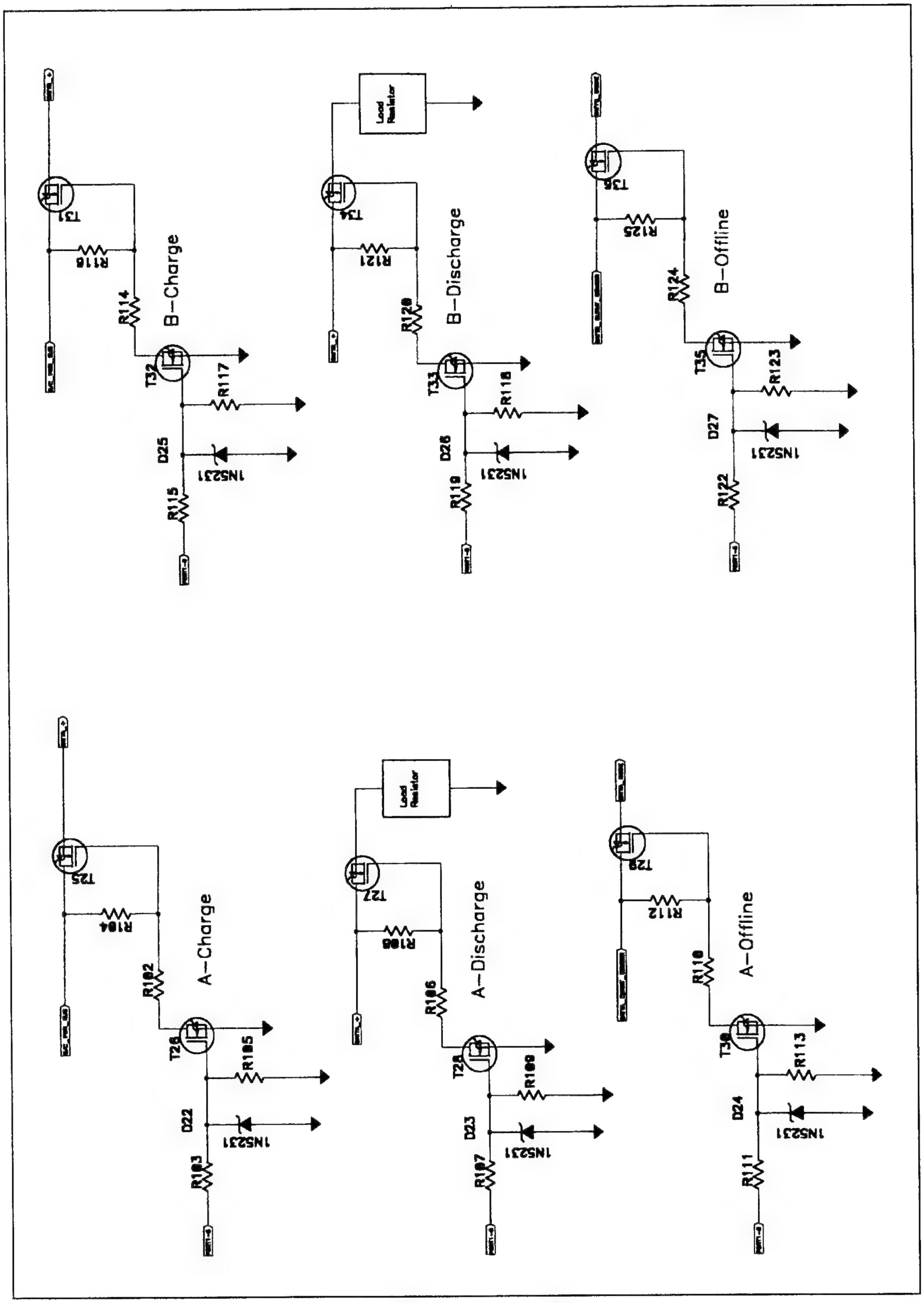


Figure A.4 EPS Electronic Power Switching Circuits

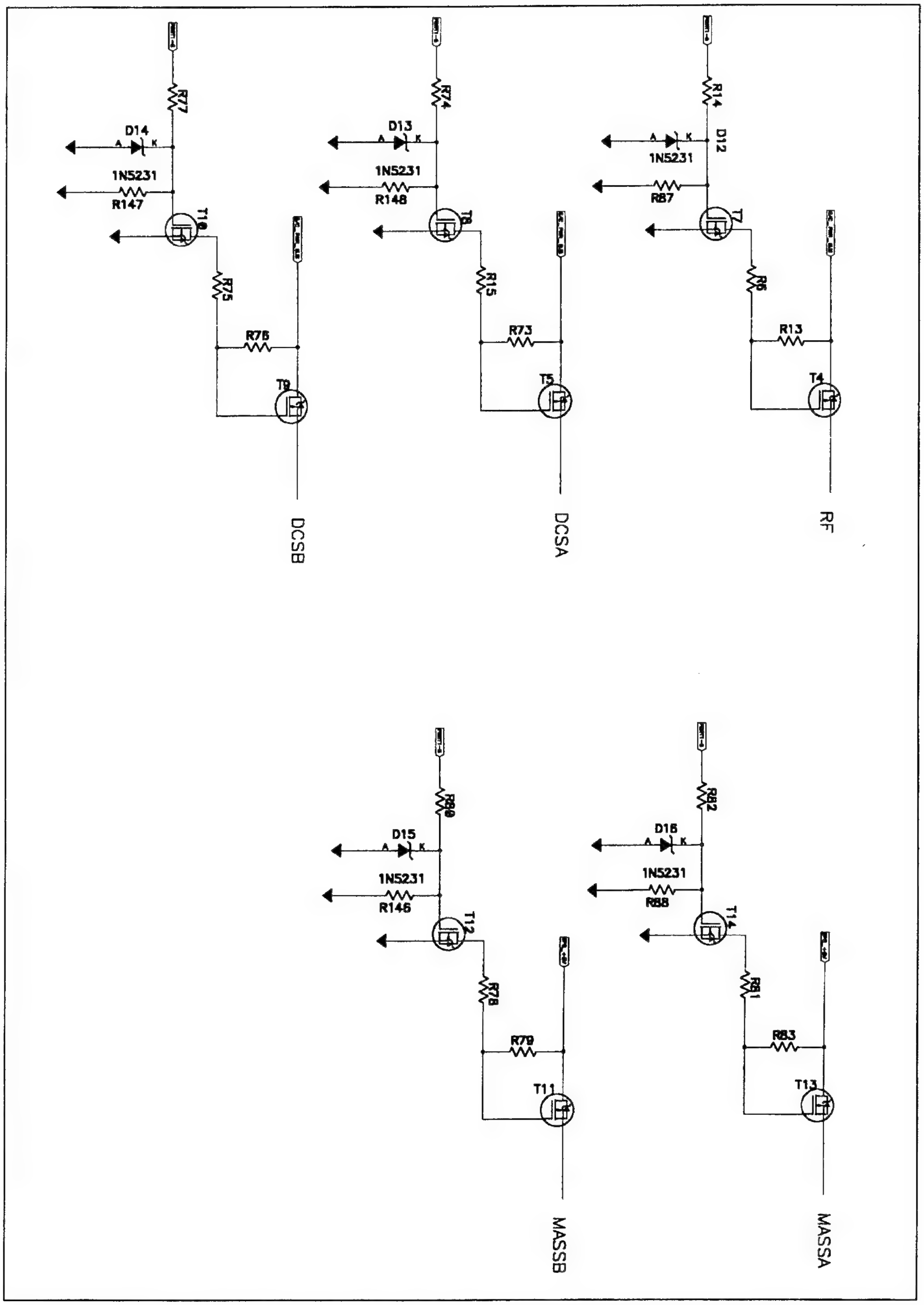


Figure A.5 EPS Electronic Power Switching Circuits (continued)

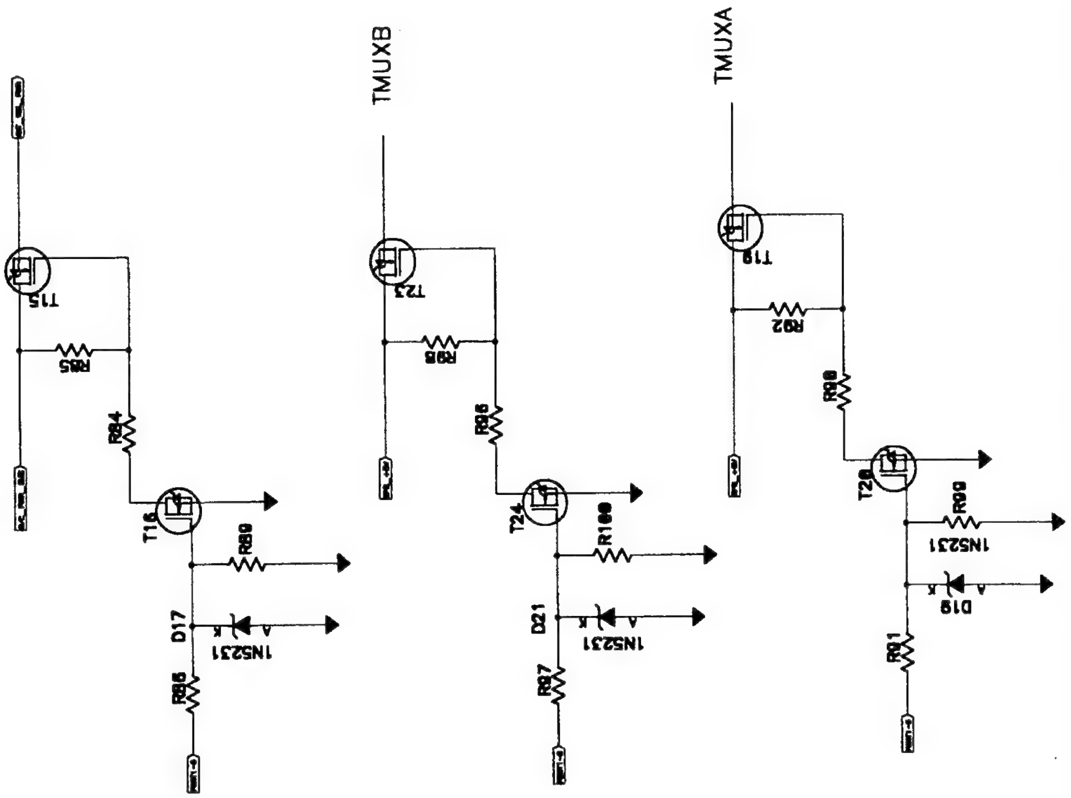


Figure A.6 EPS Electronic Power Switching Circuits (continued)

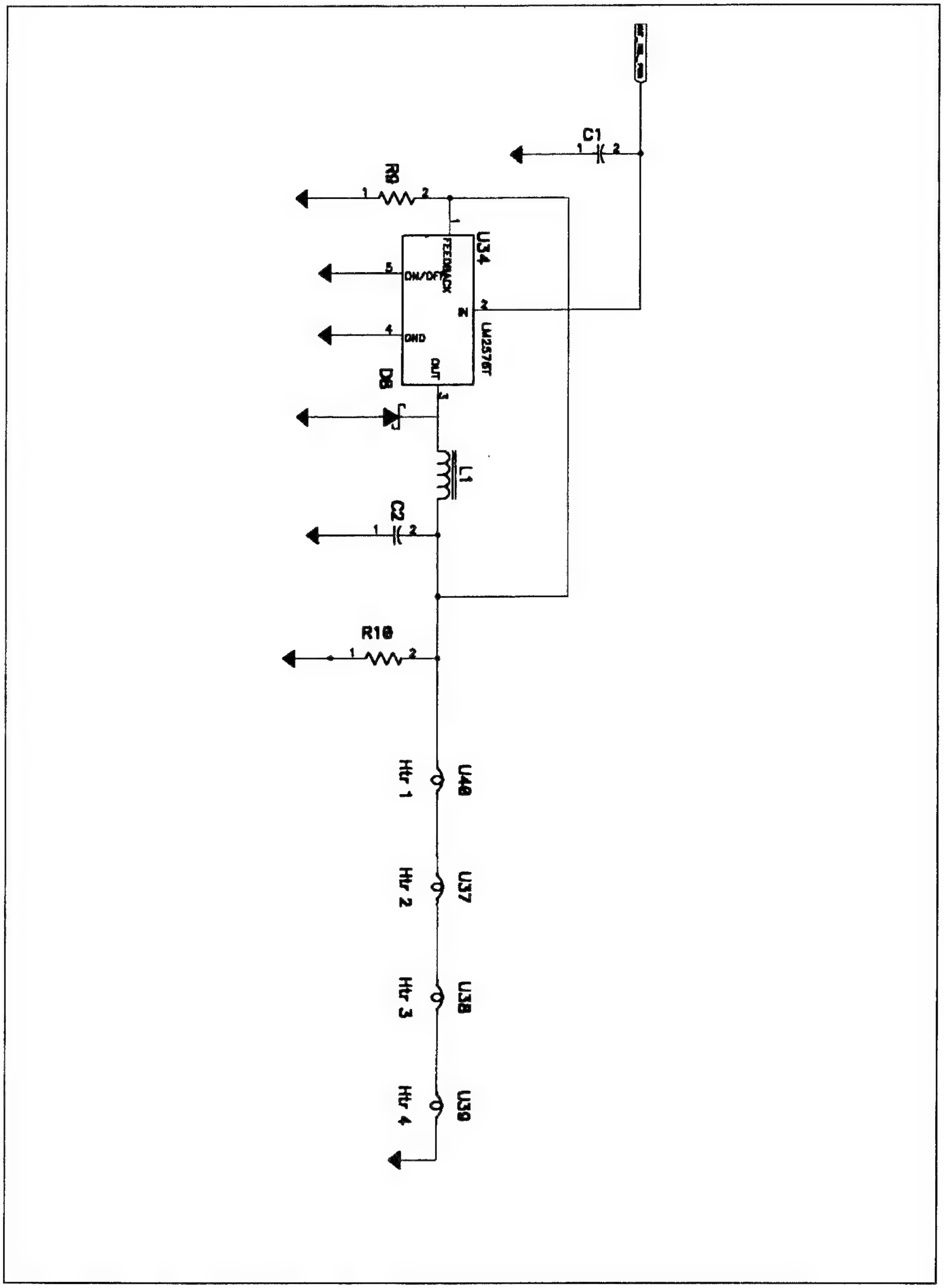


Figure A.7 Antenna Deployment Circuit

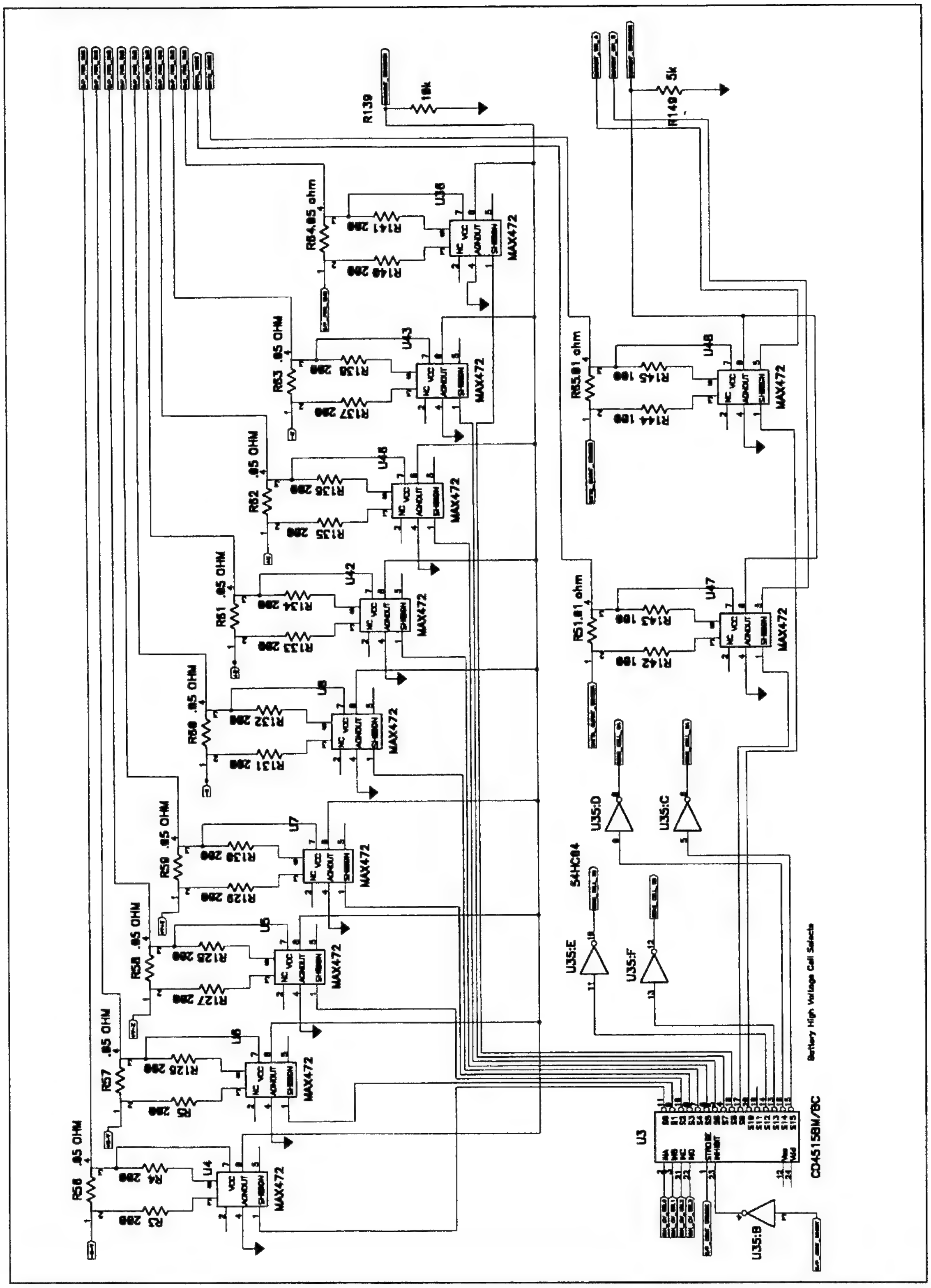


Figure A.8 EPS Current Sensing Circuit

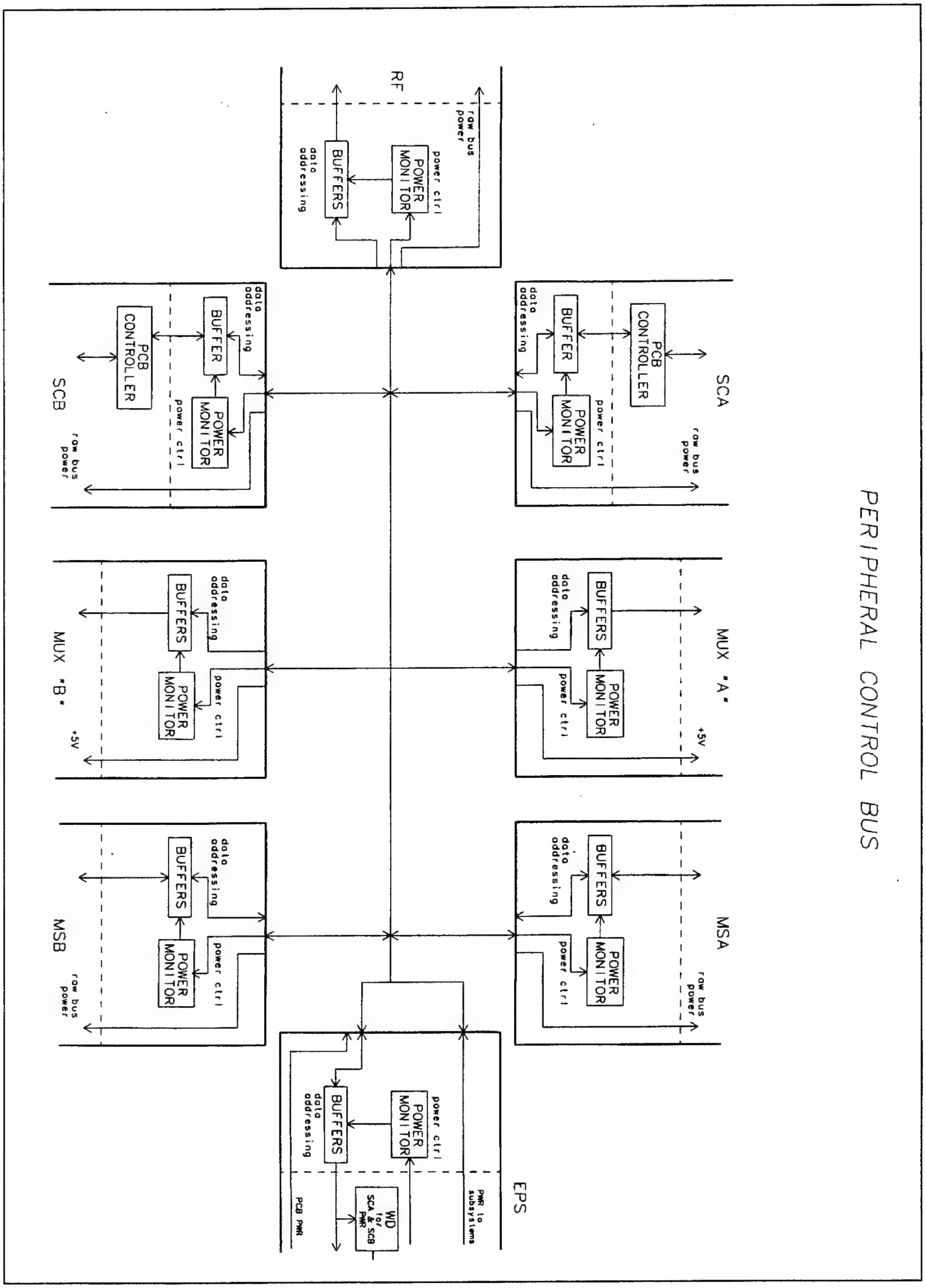


Figure A.9 Peripheral Control Bus (PCB) Diagram

Event	Description	Notes
1.1	Experimental Current Sensor Failure	A current sensor is located between the solar panel and the launch switches for each of the 8 solar panels in the solar panel illumination experiment (SPIE).
1.2	Experimental Connection Broken	Broken power connection from an SPIE solar panel to the raw power bus.
1.3	Experimental Line 1 SP Fuse Blows	Blown line 1 fuse at the SPIE solar panel end (connection of each solar panel is made with two separate lines, with each line having two fuses, one at the solar panel end and one at the EPS raw bus end).
1.4	Experimental Line 1 EPS Fuse Blows	Blown line 1 fuse at the SPIE EPS end.
1.5	Experimental Line 2 SP Fuse Blows	Blown line 2 fuse at the SPIE solar panel end.
1.6	Experimental Line 2 EPS Fuse Blows	Blown line 2 fuse at the SPIE EPS end.
1.7	Experimental S/P Blocking Diode Fails Open	Each SPIE solar panel has a blocking diode connecting the solar panel to the EPS raw power bus to prevent reverse current flow through a non-power producing solar panel. If the diode fails open then no power would be available from the solar panel.
1.8	Experimental Panel String Broken	Each SPIE solar panel consist of 32 series connected solar cells. If the connections between the cells or a cell fails open then the solar panel is ineffective.
1.9	Connection Broken	Same as 1.2 for remaining solar panels.
1.10	Line 1 SP Fuse Blows	Same as 1.3 for remaining solar panels.
1.11	Line 1 EPS Fuse Blows	Same as 1.4 for remaining solar panels.
1.12	Line 2 SP Fuse Blows	Same as 1.5 for remaining solar panels.
1.13	Line 2 EPS Fuse Blows	Same as 1.6 for remaining solar panels.
1.14	Solar Panel Blocking Diode Fails Open	Same as 1.7 for remaining solar panels.
1.15	Panel String Broken	Same as 1.8 for remaining solar panels.
1.16	S1 Failed	Launch switch connecting the solar panels and batteries to the raw power bus.
1.17	S13 Failure	Launch switch connecting the solar panels and batteries to the raw power bus.
1.18	S14 Failure	Launch switch connecting the solar panels and batteries to the raw power bus.

Event	Description	Notes
1.19	S2 Failed	Launch switch connecting the solar panels and batteries to the raw power bus.
1.20	Batt A Cell Inter-connection Broken	Broken connection between the 10 series connected type D Ni-Cd battery cells comprising battery A.
1.21	Batt A Cell Internal Connection Broken	Broken power connection internal to each type D Ni-Cd cell (e.g., between battery plates and the cell terminals).
1.22	Batt A Cell Reversal	Battery cell condition where the cell becomes a power load and causes cell polarity reversal.
1.23	Batt A Plate Degradation	Battery cell plate degradation to point the cell is not able to hold a charge.
1.24	Faulty Temp Sensing System (TMUX)	A temperature sensing circuit failure could cause a battery over temperature condition. If the temperature becomes high enough battery explosion or pressure seal blow-by could occur.
1.25	Improper Passive Thermal Control	Battery box thermal conditions exceed expected conditions due to improper passive thermal control and cause event conditions of 1.24.
1.26	Insufficient Operator Action	Ground control operation fail to take timely actions to correct improper battery thermal conditions causing high temperature operations (this may be a flag to a separate event failure).
1.27	Batt A Improper Charge Rates	If batteries are not maintained in accordance with operating specifications for charging and discharging rates, then battery life could be severely shortened.
1.28	Substandard seal construction	Poor battery seal could cause leakage or electrolyte blow-by during battery gassing evolutions and evaporation causing cell dryout (failure).
1.29	Battery Monitor Failure	If battery monitor fails to maintain an effective status measurement of battery conditions then continuous battery over-charge cycles will reduce battery lifetime
1.30	Blocking Diode D9 Fails Open	Battery A has two output blocking diodes (parallel redundancy) to prevent uncontrolled battery charging. Failure of blocking diodes will prevent placing battery on service.
1.31	Blocking Diode D20 Fails Open	See event 1.30
1.32	Battery "A" Current	Current sensor failure could prevent current flow

Event	Description	Notes
	Sensor Failure	from battery to raw power bus.
1.33	Batt B Cell Interconnection Broken	See 1.20
1.34	Batt B Cell Internal Connection Broken	See 1.21
1.35	Sub-standard Seal Construction	See 1.28
1.36	Batt B Cell Reversal	See 1.22
1.37	Batt B Plate Degradation	See 1.23
1.38	Batt B Improper Charge Rates	See 1.27
1.39	Battery Monitor Failure	See 1.29
1.40	Battery "B" Current Sensor Failure	See 1.32
1.41	Blocking Diode D10 Fails Open	See 1.30
1.42	Blocking Diode D28 Fails Open	See 1.31
1.43	Current/Voltage Sensing Ckt Failure U25/U26	Failure would cause the inability to monitor cell voltages and battery condition (see 1.29).
1.44	Batt A Charge Switch Fails Shut	Charge switch failing shut would cause continuous battery charging eventually leading to a battery over-temperature condition.
1.45	Batt B Charge Switch Fails Shut	See 1.44
1.46	D11 Fails Open	Each charge switch has two parallel diodes on the charge switch battery output side. Diode failure prevents recharging battery A.
1.47	D29 Fails Open	See 1.46
1.48	Broken Connection	Power bus failure between switch and the bus.
1.49	Batt A Chg Switch Input Fuse Failure	Each switch is fused on the input (power line side). Fuse failure prevent current flow through the switch.
1.50	Loss of +5 V from PCB to Batt A Chg Control	No control power for switch operations.
1.51	Batt A Chg Switch Component Failure	The electronic switches consists of several discrete components. Failure of most any of them will cause

Event	Description	Notes
		the switch to fail.
1.52	Batt A Discharge Switch Fails Shut	Battery continuously discharges (not able to be charged although could be taken off line).
1.53	Batt A Charge Switch Fail Shut	See 1.45
1.54	Batt A Discharge Switch Fail Shut	See 1.52
1.55	D18 Fails Open	Each charge switch has two parallel diodes on the charge switch battery output side. Diode failure prevents recharging battery B.
1.56	D30 Fails Open	See 1.55
1.57	Broken Connection	See 1.48
1.58	Input Fuse Blows	See 1.49
1.59	Loss of +5 V from PCB to Batt B Chg Control	See 1.50
1.60	Batt B Chg Switch Component Failure	See 1.51
1.61	Batt B Discharge Switch Fails Shut	See 1.52
1.62	Batt B Charge Switch Fail Shut	See 1.53
1.63	Batt B Discharge Switch Fail Shut	See 1.52
1.64	Broken Connection	See 1.48
1.65	Input Fuse Blows	See 1.49
1.66	Loss of +5 V from PCB to S3 Control	See 1.50
1.67	Batt A On-line (S3) Component Failure	Failure prevents placing battery A on-line.
1.68	Broken Connection	See 1.48
1.69	Input Fuse Blows	See 1.49
1.70	Loss of +5 V from PCB to S4 Control	See 1.50
1.71	Batt B On-line Switch (S4) Component Failure	See 1.67
1.72	Broken Data	Broken bus from the PCB wire bundle to the EPS

Event	Description	Notes
	Line/Connection	logic board addressing register U17.
1.73	PCB Interface Failure U17	Failure prevents addressing and control of EPS switches.
1.74	Loss of +5 V from PCB to Battery Control	
1.75	P/S Contingency Redundancy Failure	A failure of one +5 Volt power supply could cause the failure of the redundant power supply.
1.76	P/S "A" Failure	Failure of one +5 Volt power supply.
1.77	P/S "B" Failure	Failure of the redundant +5 Volt power supply.
1.78	PCB Failure	PCB failure causing loss of +5 Volt bus to a subsystem or component.
1.79	Interconnection Failure	PCB connection failure from bus to respective subsystem.
1.80	Blown/Faulty Fuse	Each +5 Volt power supply are fused at the input to regulating circuit.
1.81	Input Filter Failure	The +5 Volt power supply contains an input filter from the raw bus to the regulating circuits.
1.82	Output Filter Failure	There is a common +5 Volt output filter from the power supplies to the +5 Volt power bus.
1.83	Master Current Sensor Failure	Current sensor located between launch switches and raw power bus. Failure could prevent power from any source to be distributed to the loads.
1.84	Loss of +5 V from PCB	No power from the +5 Volt bus to the low threshold detector circuit, forcing the detector output low.
1.85	Low Threshold Detector Fails Low	Detector failing low would prevent resetting WDT.
1.86	Broken Connection (PCB)	PCB cable failure preventing power distribution to other subsystems.
1.87	PCB Interface Failure (U17)	See 1.73
1.88	PCB Bus/Connection Fault	Loss of command signaling to EPS components due to bus or connection failure.
1.89	PCB Interface "U18" Failure	This is a command signal register. Failure would also prevent resetting WDT.
1.90	Loss of +5 V from PCB to PCB Interface Ckts	No power from +5 Volt bus to PCB interface ckt on EPS logic board.

Event	Description	Notes
1.91	Bit Flop in Route	Incorrect command signal received at signal destination due to a bit flop in-route.
1.92	DCS Addressing Error	Incorrect command signal address sent by DCS causing no (or incorrect) operations. Could be a critical failure.
1.93	Logic Circuit "U21"	Register failure prevents all battery operations (both batteries A and B).
1.94	Logic Circuit "U22"	Register failure prevents RF, TMUX, MASS, and antenna release power switch operations.
1.95	Command Bus Failure (broken conn)	Broken bus connection between U17 and U21 (and/or U22) or from U21/U22 to the power switches.
1.96	U32:A Failure	Prevents clocking register U21.
1.97	U20:A Failure	Prevents clocking registers U21 and U22.
1.98	U19 Failure	Prevents clocking registers U21 and U22.
1.99	U31:D Failure	Prevents clocking register U22.
1.100	U20:A Failure	Prevents clocking registers U21 and U22.
1.101	U19 Failure	Prevents clocking registers U21 and U22.
1.102	U17 Failure	See 1.73
1.103	U18 Failure	See 1.89
1.104	PCB Bus/Connection Fault	Prevents command signal pass to switches if power from the PCB is lost the logic registers.
1.105	U27:A Q (Pin 5) fails High	Supplies signal to switch to energize DCS A continuously.
1.106	U27:A Q bar (Pin 6) fails High	Supplies signal to switch to energize DCS B continuously.
1.107	U27:A Q (Pin 5) Fails Low	Prevents signal switching to energize DCS A.
1.108	U27:A Q bar (Pin 6) Fails Low	Prevents signal switching to energize DCS B.
1.109	Loss of +5 V from PCB to U27:A	Cause U27:A outputs (Q and Q bar) to fail low, preventing power from being applied to either DCS A or DCS B.
1.110	P/S Contingency Redundancy Failure	See 1.75
1.111	P/S "A" Failure	See 1.76

Event	Description	Notes
1.112	P/S "B" Failure	See 1.77
1.113	PCB Failure	See 1.78
1.114	Interconnection Failure	See 1.79
1.115	Blown/Faulty Fuse	See 1.80
1.116	Input Filter Failure	See 1.81
1.117	Output Filter Failure	See 1.82
1.118	Loss of +5 V from PCB to Low Threshold Ckt	Cause low threshold detector to fail low (see 1.85).
1.119	PCB Broken Connection	Unable to reset WDT from DCS due to PCB command signaling bus failure.
1.120	PCB Interface "U18" Failure	See 1.89
1.121	Loss of +5 V from PCB to PCB Interface Ckts	See 1.90
1.122	WDT "U28" Failure	U28:C failure prevents resetting WDT with DCS rese signal.
1.123	WDT "U20" Failure	U20:B failure prevents resetting WDT with DCS rese signal.
1.124	WDT "U1" Failure	Unable to reset WDT, operating DCS remains powered until DCS or power failure secures power to the DCS. Unable to recover.
1.125	Loss of +5 V from PCB to Logic Ckts	
1.126	High Threshold Detector (>4 Volts)	High threshold detector signal failing high will clear all logic registers and U27:A, causing a loss of power to both DCS A and B.
1.127	Loss of +5 V from PCB to Low Threshold Ckt	See 1.118
1.128	WDT "U27" Failure	U27:A failure could secure power to one or both DCS subsystems. It is possible for U27:A to fail in condition at which both outputs fail high. This would both DCS subsystems to "fight" for spacecraft control
1.129	Loss of +5 V from PCB to High Threshold Ckt	
1.130	P/S Contingency Redundancy Failure	See 1.75

Event	Description	Notes
1.131	P/S "A" Failure	See 1.76
1.132	P/S "B" Failure	See 1.77
1.133	PCB Failure	See 1.78
1.134	Interconnection Failure	See 1.79
1.135	Blown/Faulty Fuse	See 1.80
1.136	Input Filter Failure	See 1.81
1.137	Output Filter Failure	See 1.82
1.138	Loss of +5 V from PCB to WDT Timing Ckt	Loss of power to U1 prevents resetting WDT (see 1.122).
1.250	Low Threshold Detector Fails Low	See 1.85

Table A.1 Electrical Power Subsystem Critical Failure Events

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
1	1 event	CIRCLE	1.1	Experimental Current Sensor Failure
2	1 event	CIRCLE	1.7	Experimental S/P Blocking Diode Fails Open
3	1 event	CIRCLE	1.8	Experimental Panel String Broken
4	1 event	CIRCLE	1.14	Solar Panel Blocking Diode Fails Open
5	1 event	CIRCLE	1.15	Panel String Broken
6	1 event	DIAMOND	1.24	Faulty Temp Sensing System (TMUX)
7	1 event	DIAMOND	1.25	Improper Passive Thermal Control
8	1 event	DIAMOND	1.26	Insufficient Operator Action
9	1 event	DIAMOND	1.39	Battery Monitor Failure
10	1 event	DIAMOND	1.43	Current/Voltage Sensing Ckt Failure U25/U26
11	1 event	DIAMOND	1.110	P/S Contingency Redundancy Failure
12	1 event	DIAMOND	1.113	PCB Failure
13	1 event	CIRCLE	1.114	Interconnection Failure
14	1 event	CIRCLE	1.115	Blown/Faulty Fuse
15	1 event	DIAMOND	1.116	Input Filter Failure
16	1 event	DIAMOND	1.117	Output Filter Failure
17	1 event	DIAMOND	1.118	Loss of +5 V from PCB to Low Threshold Ckt
18	1 event	CIRCLE	1.250	Low Threshold Detector Fails Low
19	1 event	CIRCLE	1.119	PCB Broken Connection
20	1 event	CIRCLE	1.120	PCB Interface "U18" Failure
21	1 event	DIAMOND	1.121	Loss of +5 V from PCB to PCB Interface Ckts
22	1 event	CIRCLE	1.122	WDT "U28" Failure
23	1 event	CIRCLE	1.123	WDT "U20" Failure
24	1 event	CIRCLE	1.124	WDT "U1" Failure
25	1 event	DIAMOND	1.125	Loss of +5 V from PCB to Logic Ckts
26	1 event	CIRCLE	1.126	High Threshold Detector (>4 Volts)
27	1 event	CIRCLE	1.128	WDT "U27" Failure
28	1 event	DIAMOND	1.129	Loss of +5 V from PCB to High Threshold Ckt
29	1 event	DIAMOND	1.138	Loss of +5 V from PCB to WDT Timing Ckt
30	1 event	DIAMOND	1.109	Loss of +5 V from PCB to U27:A
31	1 event	DIAMOND	1.83	Master Current Sensor Failure

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
32	1 event	DIAMOND	1.84	Loss of +5 V from PCB
33	1 event	DIAMOND	1.86	Broken Connection (PCB)
34	1 event	CIRCLE	1.87	PCB Interface Failure (U17)
35	1 event	CIRCLE	1.88	PCB Bus/Connection Fault
36	1 event	DIAMOND	1.91	Bit Flop in Route
37	1 event	DIAMOND	1.92	DCS Addressing Error
38	1 event	CIRCLE	1.93	Logic Circuit "U21"
39	1 event	CIRCLE	1.94	Logic Circuit "U22"
40	1 event	CIRCLE	1.95	Command Bus Failure (broken conn)
41	1 event	CIRCLE	1.96	U32:A Failure
42	1 event	CIRCLE	1.97	U20:A Failure
43	1 event	CIRCLE	1.98	U19 Failure
44	1 event	CIRCLE	1.99	U31:D Failure
45	1 event	CIRCLE	1.102	U17 Failure
46	1 event	CIRCLE	1.103	U18 Failure
47	2 events	CIRCLE	1.17	S13 Failure
		CIRCLE	1.16	S1 Failed
48	2 events	CIRCLE	1.18	S14 Failure
		CIRCLE	1.16	S1 Failed
49	2 events	CIRCLE	1.17	S13 Failure
		CIRCLE	1.19	S2 Failed
50	2 events	CIRCLE	1.18	S14 Failure
		CIRCLE	1.19	S2 Failed
51	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		CIRCLE	1.33	Batt B Cell Interconnection Broken
52	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		CIRCLE	1.33	Batt B Cell Interconnection Broken
53	2 events	DIAMOND	1.22	Batt A Cell Reversal
		CIRCLE	1.33	Batt B Cell Interconnection Broken
54	2 events	DIAMOND	1.23	Batt A Plate Degradation
		CIRCLE	1.33	Batt B Cell Interconnection Broken

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
55	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		CIRCLE	1.33	Batt B Cell Interconnection Broken
56	2 events	CIRCLE	1.28	Substandard seal construction
		CIRCLE	1.33	Batt B Cell Interconnection Broken
57	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		CIRCLE	1.33	Batt B Cell Interconnection Broken
58	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
59	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
60	2 events	DIAMOND	1.22	Batt A Cell Reversal
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
61	2 events	DIAMOND	1.23	Batt A Plate Degradation
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
62	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
63	2 events	CIRCLE	1.28	Substandard seal construction
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
64	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
65	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		CIRCLE	1.35	Sub-standard Seal Construction
66	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		CIRCLE	1.35	Sub-standard Seal Construction
67	2 events	DIAMOND	1.22	Batt A Cell Reversal
		CIRCLE	1.35	Sub-standard Seal Construction
68	2 events	DIAMOND	1.23	Batt A Plate Degradation
		CIRCLE	1.35	Sub-standard Seal Construction
69	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		CIRCLE	1.35	Sub-standard Seal Construction
70	2 events	CIRCLE	1.28	Substandard seal construction

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
		CIRCLE	1.35	Sub-standard Seal Construction
71	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		CIRCLE	1.35	Sub-standard Seal Construction
72	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		DIAMOND	1.36	Batt B Cell Reversal
73	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		DIAMOND	1.36	Batt B Cell Reversal
74	2 events	DIAMOND	1.22	Batt A Cell Reversal
		DIAMOND	1.36	Batt B Cell Reversal
75	2 events	DIAMOND	1.23	Batt A Plate Degradation
		DIAMOND	1.36	Batt B Cell Reversal
76	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		DIAMOND	1.36	Batt B Cell Reversal
77	2 events	CIRCLE	1.28	Substandard seal construction
		DIAMOND	1.36	Batt B Cell Reversal
78	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		DIAMOND	1.36	Batt B Cell Reversal
79	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		DIAMOND	1.37	Batt B Plate Degradation
80	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		DIAMOND	1.37	Batt B Plate Degradation
81	2 events	DIAMOND	1.22	Batt A Cell Reversal
		DIAMOND	1.37	Batt B Plate Degradation
82	2 events	DIAMOND	1.23	Batt A Plate Degradation
		DIAMOND	1.37	Batt B Plate Degradation
83	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		DIAMOND	1.37	Batt B Plate Degradation
84	2 events	CIRCLE	1.28	Substandard seal construction
		DIAMOND	1.37	Batt B Plate Degradation
85	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		DIAMOND	1.37	Batt B Plate Degradation

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
86	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		DIAMOND	1.38	Batt B Improper Charge Rates
87	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		DIAMOND	1.38	Batt B Improper Charge Rates
88	2 events	DIAMOND	1.22	Batt A Cell Reversal
		DIAMOND	1.38	Batt B Improper Charge Rates
89	2 events	DIAMOND	1.23	Batt A Plate Degradation
		DIAMOND	1.38	Batt B Improper Charge Rates
90	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		DIAMOND	1.38	Batt B Improper Charge Rates
91	2 events	CIRCLE	1.28	Substandard seal construction
		DIAMOND	1.38	Batt B Improper Charge Rates
92	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		DIAMOND	1.38	Batt B Improper Charge Rates
93	2 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		DIAMOND	1.40	Battery "B" Current Sensor Failure
94	2 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		DIAMOND	1.40	Battery "B" Current Sensor Failure
95	2 events	DIAMOND	1.22	Batt A Cell Reversal
		DIAMOND	1.40	Battery "B" Current Sensor Failure
96	2 events	DIAMOND	1.23	Batt A Plate Degradation
		DIAMOND	1.40	Battery "B" Current Sensor Failure
97	2 events	DIAMOND	1.27	Batt A Improper Charge Rates
		DIAMOND	1.40	Battery "B" Current Sensor Failure
98	2 events	CIRCLE	1.28	Substandard seal construction
		DIAMOND	1.40	Battery "B" Current Sensor Failure
99	2 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		DIAMOND	1.40	Battery "B" Current Sensor Failure
100	2 events	DIAMOND	1.112	P/S "B" Failure
		DIAMOND	1.111	P/S "A" Failure
101	2 events	CIRCLE	1.106	U27:A Q bar (Pin 6) fails High

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
		CIRCLE	1.105	U27:A Q (Pin 5) fails High
102	2 events	CIRCLE	1.108	U27:A Q bar (Pin 6) Fails Low
		CIRCLE	1.107	U27:A Q (Pin 5) Fails Low
103	3 events	CIRCLE	1.3	Experimental Line 1 SP Fuse Blows
		CIRCLE	1.5	Experimental Line 2 SP Fuse Blows
		CIRCLE	1.2	Experimental Connection Broken
104	3 events	CIRCLE	1.4	Experimental Line 1 EPS Fuse Blows
		CIRCLE	1.5	Experimental Line 2 SP Fuse Blows
		CIRCLE	1.2	Experimental Connection Broken
105	3 events	CIRCLE	1.3	Experimental Line 1 SP Fuse Blows
		CIRCLE	1.6	Experimental Line 2 EPS Fuse Blows
		CIRCLE	1.2	Experimental Connection Broken
106	3 events	CIRCLE	1.4	Experimental Line 1 EPS Fuse Blows
		CIRCLE	1.6	Experimental Line 2 EPS Fuse Blows
		CIRCLE	1.2	Experimental Connection Broken
107	3 events	CIRCLE	1.10	Line 1 SP Fuse Blows
		CIRCLE	1.12	Line 2 SP Fuse Blows
		CIRCLE	1.9	Connection Broken
108	3 events	CIRCLE	1.11	Line 1 EPS Fuse Blows
		CIRCLE	1.12	Line 2 SP Fuse Blows
		CIRCLE	1.9	Connection Broken
109	3 events	CIRCLE	1.10	Line 1 SP Fuse Blows
		CIRCLE	1.13	Line 2 EPS Fuse Blows
		CIRCLE	1.9	Connection Broken
110	3 events	CIRCLE	1.11	Line 1 EPS Fuse Blows
		CIRCLE	1.13	Line 2 EPS Fuse Blows
		CIRCLE	1.9	Connection Broken
111	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		CIRCLE	1.33	Batt B Cell Interconnection Broken
112	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		CIRCLE	1.34	Batt B Cell Internal Connection Broken
113	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		CIRCLE	1.35	Sub-standard Seal Construction
114	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		DIAMOND	1.36	Batt B Cell Reversal
115	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		DIAMOND	1.37	Batt B Plate Degradation
116	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		DIAMOND	1.38	Batt B Improper Charge Rates
117	3 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		DIAMOND	1.40	Battery "B" Current Sensor Failure
118	3 events	CIRCLE	1.20	Batt A Cell Interconnection Broken
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
119	3 events	CIRCLE	1.21	Batt A Cell Internal Connection Broken
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
120	3 events	DIAMOND	1.22	Batt A Cell Reversal
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
121	3 events	DIAMOND	1.23	Batt A Plate Degradation
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
122	3 events	DIAMOND	1.27	Batt A Improper Charge Rates
		CIRCLE	1.42	Blocking Diode D28 Fails Open

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
		CIRCLE	1.41	Blocking Diode D10 Fails Open
123	3 events	CIRCLE	1.28	Substandard seal construction
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
124	3 events	DIAMOND	1.32	Battery "A" Current Sensor Failure
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open
125	4 events	CIRCLE	1.31	Blocking Diode D20 Fails Open
		CIRCLE	1.30	Blocking Diode D9 Fails Open
		CIRCLE	1.42	Blocking Diode D28 Fails Open
		CIRCLE	1.41	Blocking Diode D10 Fails Open

Table A.2 Electrical Power Subsystem Minimum Cut Sets

APPENDIX B. RF SUBSYSTEM

FAULT TREE ANALYSIS

This appendix contains the raw data for the FTA of the RF subsystem. Figure B.1 is a block diagram of the RF subsystem and Fig. B.2 is a depiction of the antenna assembly. The RF failure end events are listed in table B.1 with a brief description. Table B.2 list the minimum cut sets for the RF system generated by the FaultrEASE software program for the PANSAT fault tree in Appendix D.

The minimum cut sets were generated using a direct evaluation technique employed by the software package. The basic end events were compared by their description label contents.

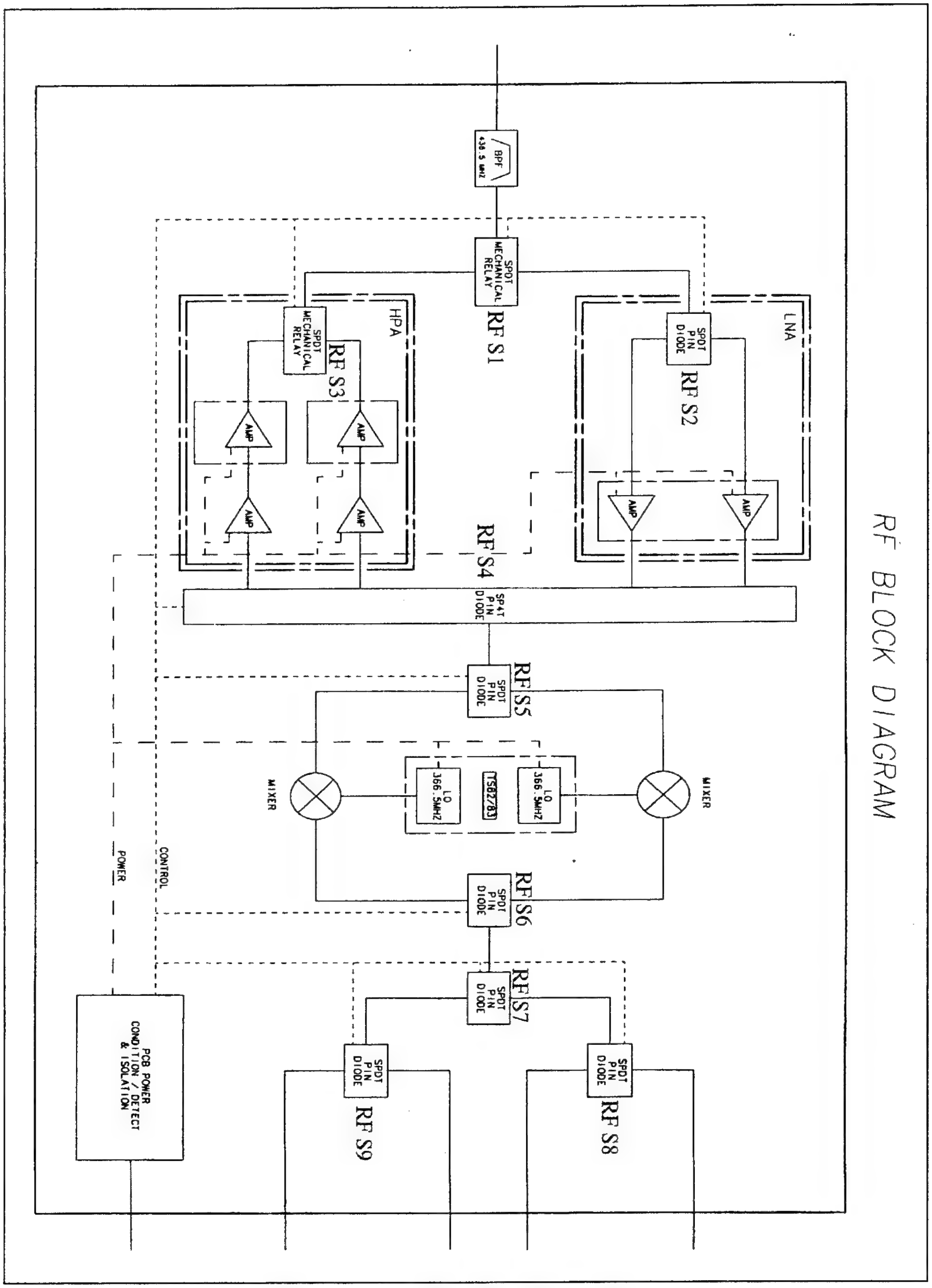


Figure B.1 RF Subsystem Block Diagram

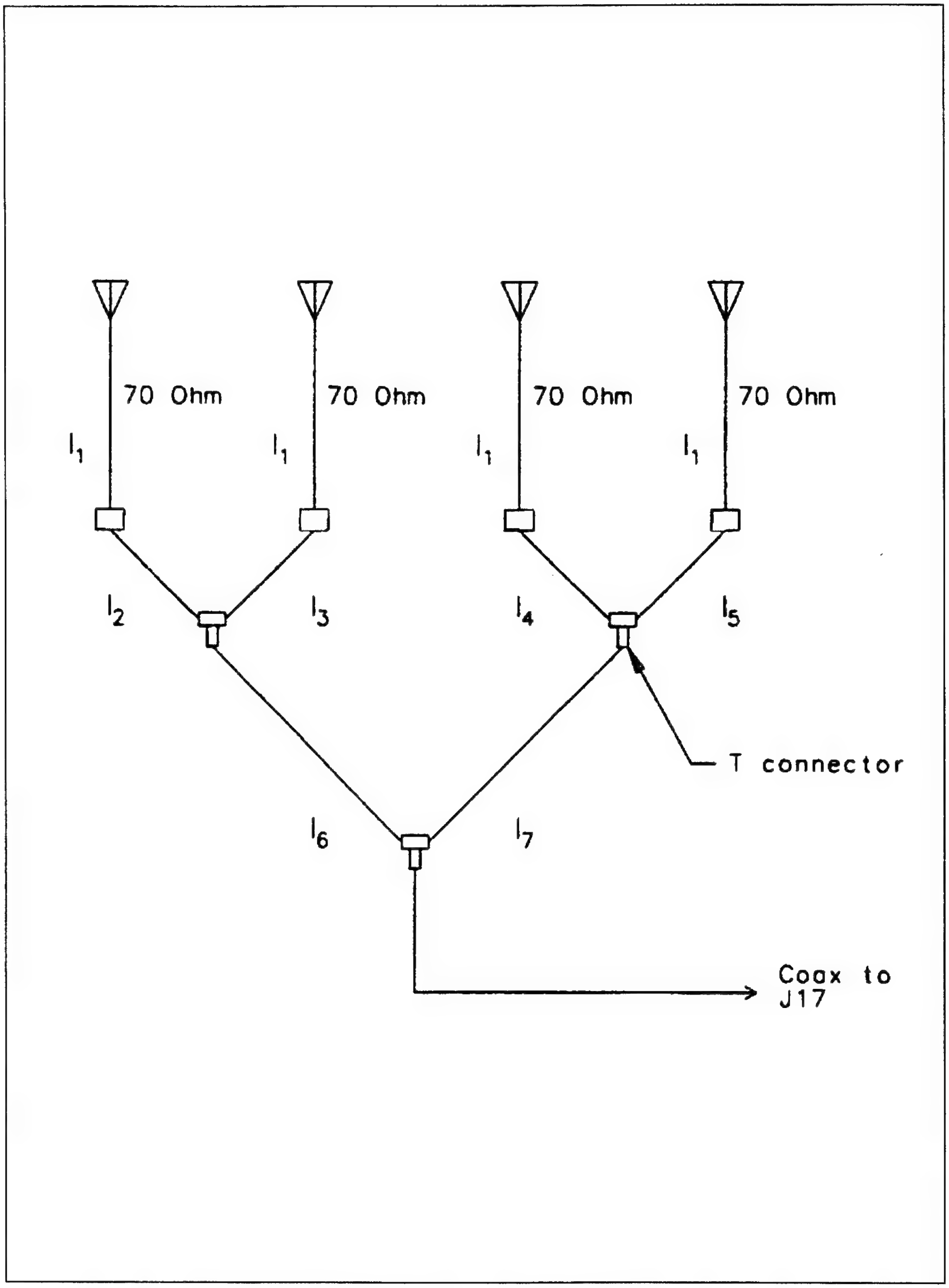


Figure B.2 Antenna System

Event	End Event Failure	Notes
2.1	Broken Connection	Refers to broken connection between PCB and PCB interface ckt
2.2	PCB Interface Failure	Failure prevents power to RF components
2.3	P/S Contingency Redundancy Failure	Refers to a of one +5 Volt power supplies causing a failure in the second (stand by) +5 Volt power supplies. This is possible with current design.
2.4	P/S "A" Failure	Failure of one +5 Volt power supplies (listed as power supply A)
2.5	P/S "B" Failure	Failure of second +5 Volt power supplies (listed as power supply B)
2.6	PCB Failure	Failure of PCB cabling in distribution of +5 Volt
2.7	Interconnection Failure	Failure of PCB connectors
2.8	Blown/Faulty Fuse	Failure of +5 Volt P/S input fuses
2.9	Input Filter Failure	Failure of +5 Volt P/S line filter from raw power bus
2.10	Output Filter Failure	Failure of +5 Volt P/S line filter to +5 Volt bus
2.11	Conditioning Circuit Failure	Conditions power for local use
2.12	Amp #1-1 Fail	RF Transmitter section amplifier
2.13	Amp #1-2 Fail	RF Transmitter section amplifier
2.14	Amp #2-1 Fail	RF Transmitter section amplifier
2.15	Amp #2-2 Fail	RF Transmitter section amplifier
2.16	Loss of Raw Bus Power	Loss of power to RF transmitter section
2.17	RF Switch S3 Mechanical Failure	Selects one of two cascaded HPA's, each of which contain two amplifiers
2.18	Broken Command Signaling Bus to RF S3	No command signal received at switch due to loss of conductivity between control signaling bus and the switch
2.19	DCS Command Signaling Failure to RF S3	No command signal received at switch due to incorrect command addressing logic
2.20	Loss of Power to RF S3	Loss of power for the command (control) signaling bus from the RF PCB Interface Ckt
2.21	DCS Addressing Error to RF S3	Incorrect command signal received at switch due to invalid addressing logic
2.22	Bit Flop in Route to Switch to RF S3	Incorrect command signal received at switch due to an address or command signal bit flop

Event	End Event Failure	Notes
		in-route from the DCS to the switch
2.23	Power Surge to RF S3	Incorrect command signal received at the switch due to a power surge on the command bus.
2.24	RF S9 Switch Mechanical Failure	Selects which DCS transmitter section the RF transmitter will be connected. One possible failure is if the switch was two fail in mid position
2.25	Broken Command Signaling Bus to RF S9	
2.26	DCS Command Signaling Failure to RF S9	
2.27	Loss of Power to RF S9	
2.28	DCS Addressing Error to RF S9	
2.29	Bit Flop in Route to Switch to RF S9	
2.30	Power Surge to RF S9	
2.31	RF S2 Switch Mechanical Failure	Switch selects one of two independent LNA's
2.32	Broken Command Signaling Bus to RF S2	Broken command signaling conductivity prevents commanding and control of switches
2.33	DCS Command Signaling Failure to RF S2	Failure of command signal from
2.34	Loss of Power to RF S2	
2.35	DCS Addressing Error to RF S2	Incorrect or inadvertent switch address sent to EPS logic ckt
2.36	Bit Flop in Route to Switch to RF S2	Incorrect command signal at switch control due to bit error in-route
2.37	Power Surge to RF S2	
2.38	RF S2 Switch Power Failure	
2.39	LNA #1 Component Failure	Failure prevents amplification of receive DSSS signal
2.40	Loss of Raw Bus Power to LNA #1	
2.41	LNA #2 Component Failure	Failure prevents amplification of receive DSSS signal

Event	End Event Failure	Notes
2.42	Loss of Raw Bus Power to LNA #2	
2.43	RF S8 Switch Mechanical Failure	Switch selects which DCS will receive message signal
2.44	Broken Command Signaling Bus to RF S8	
2.45	DCS Command Signaling Failure to RF S8	
2.46	Loss of Power to RF S8	
2.47	DCS Addressing Error to RF S8	
2.48	Bit Flop in Route to Switch to RF S8	
2.49	Power Surge to RF S8	
2.50	RF S4 Switch Mechanical Failure	Switch routes the transmit and receive signals from and to the local oscillator section
2.51	Broken Command Signaling Bus to RF S4	
2.52	DCS Command Signaling Failure to RF S4	
2.53	Loss of Power to RF S4	
2.54	DCS Addressing Error to RF S4	
2.55	Bit Flop in Route to Switch to RF S4	
2.56	Power Surge to RF S4	
2.57	High Antenna Coupling Impedance	This failure is caused by high impedance of T cou connecting the 4 dipole antennas to the coaxial cable or the connection of the coaxial cable to the BPF
2.58	Open Primary or Secondary Windings	Failure of the impedance matching transformers connecting the 4 dipole antennas to the T connectors
2.59	High Primary/Secondary Impedance	High impedance could reject or severely attenuate signal

Event	End Event Failure	Notes
2.60	Antenna T-Connector Failure (1 of 3)	Prevents signal transmission to and from antenna
2.61	Broken Coax from Feed System to BPF	Failure causes loss of conductivity between antenna and RF subsystem
2.62	Shorted Primary to Ground	Signal at antenna impedance matching transformers shorted to ground
2.63	Shorted Secondary to Ground	Signal at antenna impedance matching transformers shorted to ground
2.64	Shorted Primary to Secondary	Changes impedance coupling characteristics
2.65	Antenna T-Connector Failure (1 of 3)	
2.66	Increased Pass Bandwidth	Antenna BPF bandwidth increases (more noise passed throught BPF, lowering the signal to noise ratio
2.67	Alter Pass Band Characteristics	Increased noise (lower signal to noise ratio) due altered BPF characteristic response curve
2.68	Increased Filter Line Impedance	Signal strength decreased due to higher line impedance cause by BPF
2.69	Signal Coupled to Ground	Signal strength decreased due to failure in BPF coupling signal to ground
2.70	Broken Signal Path (filter)	Signal path broken between antenna and RF subsystem by BPF
2.71	Signal Shorted to Ground	Signal shorted to ground by BPF
2.72	T/R Switch (S1) Mechanical Failure	Switch select signals from either the HPA or LNA to the antenna
2.73	Broken Command Signaling Bus to S1	
2.74	DCS Command Signaling Failure to S1	
2.75	Loss of Command Signaling Power to S1	
2.76	DCS Addressing Error to S1	
2.77	Bit Flop in Route to Switch to S1	

Event	End Event Failure	Notes
2.78	Power Surge (transient anomaly) to S1	
2.79	Antenna Deployment Hardware Circuit Failure	
2.80	Improper Control Signal	Incorrect commanding signal from DCS to deploy the dipole antennas
2.81	Control Signal Bus Failure	Antenna deployment command signal does not reach deployment circuit due to command bus failure
2.82	Antenna Release Heater Failure	
2.83	Insufficient Solar Power	Power required to deploy antenna's
2.84	Low Battery Power	Power required to deploy antenna's (this may not be a valid failure scenerio since the battery is not relied upon as a power source for antenna deployment
2.85	Antenna Manually Fails to Release	If the antenna deployment circuit does not function, it is anticipated that the nylon cords which hold the antennas in place will eventually severe
2.86	Antenna Failure (1 of 4)	Antenna fails due to mechanical failure (e.g., broken dipole, antenna seperates from it's mounting, etc.)
2.87	Antenna Grounded	Antenna shorts signal to structure or system ground
2.88	RF S5 Switch Mechanical Failure	Switch connects a local oscillator to RF S4
2.89	Broken Command Signaling Bus to RF S5	
2.90	DCS Command Signaling Failure to RF S5	
2.91	Loss of Power to RF S5	
2.92	DCS Addressing Error to RF S5	
2.93	Bit Flop in Route to Switch to RF S5	

Event	End Event Failure	Notes
2.94	Power Surge to RF S5	
2.95	RF S6 Switch Mechanical Failure	Switch connects local oscillator to RF S7
2.96	Broken Command Signaling Bus to RF S6	
2.97	DCS Command Signaling Failure to RF S6	
2.98	Loss of Power to RF S6	
2.99	DCS Addressing Error to RF S6	
2.100	Bit Flop in Route to Switch to RF S6	
2.101	Power Surge to RF S6	
2.102	RF S7 Switch Mechanical Failure	Switch connects signal to/from RF S6 to the respective DCS transmitter and receiver sections
2.103	Broken Command Signaling Bus to RF S7	
2.104	DCS Command Signaling Failure to RF S7	
2.105	Loss of Power to RF S7	
2.106	DCS Addressing Error to RF S7	
2.107	Bit Flop in Route to Switch to RF S7	
2.108	Power Surge to RF S7	
2.109	Oscillator #1 Ckt Failure	Upshifts and downshifts transmission freq. to IF
2.110	Oscillator #1 Frequency Drift	Frequency drift could cause rejection by bandpass filters or message distortion
2.111	Mixer #1 Failure	Conducts frequency upshift and downshift
2.112	Oscillator #2 Ckt Failure	Upshifts and downshifts transmission frequency to IF
2.113	Oscillator #2 Frequency Drift	Frequency drift could cause rejection by bandpass filters or message distortion
2.114	Mixer #2 Failure	Conducts frequency upshift and downshift

Table B.1 RF Subsystem Critical End Events

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
1	1 event	DIAMOND	2.1	Broken Connection
2	1 event	DIAMOND	2.2	PCB Interface Failure
3	1 event	DIAMOND	2.3	P/S Contingency Redundancy Failure
4	1 event	DIAMOND	2.6	PCB Failure
5	1 event	CIRCLE	2.7	Interconnection Failure
6	1 event	CIRCLE	2.8	Blown/Faulty Fuse
7	1 event	DIAMOND	2.9	Input Filter Failure
8	1 event	DIAMOND	2.10	Output Filter Failure
9	1 event	DIAMOND	2.11	Conditioning Circuit Failure
10	1 event	DIAMOND	2.16	Loss of Raw Bus Power
11	1 event	CIRCLE	2.17	RF Switch S3 Mechanical Failure
12	1 event	DIAMOND	2.18	Broken Command Signaling Bus to RF S3
13	1 event	DIAMOND	2.19	DCS Command Signaling Failure to RF S3
14	1 event	DIAMOND	2.20	Loss of Power to RF S3
15	1 event	DIAMOND	2.21	DCS Addressing Error to RF S3
16	1 event	DIAMOND	2.22	Bit Flop in Route to Switch to RF S3
17	1 event	DIAMOND	2.23	Power Surge to RF S3
18	1 event	CIRCLE	2.50	RF S4 Switch Mechanical Failure
19	1 event	DIAMOND	2.51	Broken Command Signaling Bus to RF S4
20	1 event	DIAMOND	2.52	DCS Command Signaling Failure to RF S4
21	1 event	DIAMOND	2.53	Loss of Power to RF S4
22	1 event	DIAMOND	2.54	DCS Addressing Error to RF S4
23	1 event	DIAMOND	2.55	Bit Flop in Route to Switch to RF S4
24	1 event	DIAMOND	2.56	Power Surge to RF S4
25	1 event	CIRCLE	2.24	RF S9 Switch Mechanical Failure
26	1 event	DIAMOND	2.25	Broken Command Signaling Bus to RF S9
27	1 event	DIAMOND	2.26	DCS Command Signaling Failure to RF S9
28	1 event	DIAMOND	2.27	Loss of Power to RF S9
29	1 event	DIAMOND	2.28	DCS Addressing Error to RF S9
30	1 event	DIAMOND	2.29	Bit Flop in Route to Switch to RF S9
31	1 event	DIAMOND	2.30	Power Surge to RF S9

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
32	1 event	DIAMOND	2.57	High Antenna Coupling Impedance
33	1 event	CIRCLE	2.58	Open Primary or Secondary Windings
34	1 event	DIAMOND	2.59	High Primary/Secondary Impedance
35	1 event	DIAMOND	2.60	Antenna T-Connector Failure (1 of 3)
36	1 event	CIRCLE	2.61	Broken Coax from Feed System to BPF
37	1 event	CIRCLE	2.62	Shorted Primary to Ground
38	1 event	CIRCLE	2.63	Shorted Secondary to Ground
39	1 event	CIRCLE	2.64	Shorted Primary to Secondary
40	1 event	CIRCLE	2.65	Antenna T-Connector Failure (1 of 3)
41	1 event	DIAMOND	2.66	Increased Pass Bandwidth
42	1 event	DIAMOND	2.67	Alter Pass Band Characteristics
43	1 event	DIAMOND	2.68	Increased Filter Line Impedance
44	1 event	DIAMOND	2.69	Signal Coupled to Ground
45	1 event	DIAMOND	2.70	Broken Signal Path (filter)
46	1 event	DIAMOND	2.71	Signal Shorted to Ground
47	1 event	CIRCLE	2.72	T/R Switch (S1) Mechanical Failure
48	1 event	DIAMOND	2.73	Broken Command Signaling Bus to S1
49	1 event	DIAMOND	2.74	DCS Command Signaling Failure to S1
50	1 event	DIAMOND	2.75	Loss of Command Signaling Power to S1
51	1 event	DIAMOND	2.76	DCS Addressing Error to S1
52	1 event	DIAMOND	2.77	Bit Flop in Route to Switch to S1
53	1 event	DIAMOND	2.78	Power Surge (transient anomaly) to S1
54	1 event	CIRCLE	2.86	Antenna Failure (1 of 4)
55	1 event	CIRCLE	2.87	Antenna Grounded
56	1 event	CIRCLE	2.88	RF S5 Switch Mechanical Failure
57	1 event	DIAMOND	2.89	Broken Command Signaling Bus to RF S5
58	1 event	DIAMOND	2.90	DCS Command Signaling Failure to RF S5
59	1 event	DIAMOND	2.91	Loss of Power to RF S5
60	1 event	DIAMOND	2.92	DCS Addressing Error to RF S5
61	1 event	DIAMOND	2.93	Bit Flop in Route to Switch to RF S5
62	1 event	DIAMOND	2.94	Power Surge to RF S5

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
63	1 event	CIRCLE	2.95	RF S6 Switch Mechanical Failure
64	1 event	DIAMOND	2.96	Broken Command Signaling Bus to RF S6
65	1 event	DIAMOND	2.97	DCS Command Signaling Failure to RF S6
66	1 event	DIAMOND	2.98	Loss of Power to RF S6
67	1 event	DIAMOND	2.99	DCS Addressing Error to RF S6
68	1 event	DIAMOND	2.100	Bit Flop in Route to Switch to RF S6
69	1 event	DIAMOND	2.101	Power Surge to RF S6
70	1 event	CIRCLE	2.102	RF S7 Switch Mechanical Failure
71	1 event	DIAMOND	2.103	Broken Command Signaling Bus to RF S7
72	1 event	DIAMOND	2.104	DCS Command Signaling Failure to RF S7
73	1 event	DIAMOND	2.105	Loss of Power to RF S7
74	1 event	DIAMOND	2.106	DCS Addressing Error to RF S7
75	1 event	DIAMOND	2.107	Bit Flop in Route to Switch to RF S7
76	1 event	DIAMOND	2.108	Power Surge to RF S7
77	1 event	CIRCLE	2.43	RF S8 Switch Mechanical Failure
78	1 event	DIAMOND	2.44	Broken Command Signaling Bus to RF S8
79	1 event	DIAMOND	2.45	DCS Command Signaling Failure to RF S8
80	1 event	DIAMOND	2.46	Loss of Power to RF S8
81	1 event	DIAMOND	2.47	DCS Addressing Error to RF S8
82	1 event	DIAMOND	2.48	Bit Flop in Route to Switch to RF S8
83	1 event	DIAMOND	2.49	Power Surge to RF S8
84	1 event	CIRCLE	2.31	RF S2 Switch Mechanical Failure
85	1 event	DIAMOND	2.32	Broken Command Signaling Bus to RF S2
86	1 event	DIAMOND	2.33	DCS Command Signaling Failure to RF S2
87	1 event	DIAMOND	2.34	Loss of Power to RF S2
88	1 event	DIAMOND	2.35	DCS Addressing Error to RF S2
89	1 event	DIAMOND	2.36	Bit Flop in Route to Switch to RF S2
90	1 event	DIAMOND	2.37	Power Surge to RF S2
91	2 events	DIAMOND	2.5	P/S "B" Failure
		DIAMOND	2.4	P/S "A" Failure
92	2 events	DIAMOND	2.12	Amp #1-1 Fail

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
		DIAMOND	2.14	Amp #2-1 Fail
93	2 events	DIAMOND	2.13	Amp #1-2 Fail
		DIAMOND	2.14	Amp #2-1 Fail
94	2 events	DIAMOND	2.12	Amp #1-1 Fail
		DIAMOND	2.15	Amp #2-2 Fail
95	2 events	DIAMOND	2.13	Amp #1-2 Fail
		DIAMOND	2.15	Amp #2-2 Fail
96	2 events	DIAMOND	2.79	Antenna Deployment Hardware Circuit Failure
		CIRCLE	2.85	Antenna Manually Fails to Release
97	2 events	DIAMOND	2.80	Improper Control Signal
		CIRCLE	2.85	Antenna Manually Fails to Release
98	2 events	DIAMOND	2.81	Control Signal Bus Failure
		CIRCLE	2.85	Antenna Manually Fails to Release
99	2 events	CIRCLE	2.82	Antenna Release Heater Failure
		CIRCLE	2.85	Antenna Manually Fails to Release
100	2 events	DIAMOND	2.83	Insufficient Solar Power
		CIRCLE	2.85	Antenna Manually Fails to Release
101	2 events	DIAMOND	2.84	Low Battery Power
		CIRCLE	2.85	Antenna Manually Fails to Release
102	2 events	DIAMOND	2.109	Oscillator #1 Ckt Failure
		DIAMOND	2.112	Oscillator #2 Ckt Failure
103	2 events	DIAMOND	2.110	Oscillator #1 Frequency Drift
		DIAMOND	2.112	Oscillator #2 Ckt Failure
104	2 events	DIAMOND	2.111	Mixer #1 Failure
		DIAMOND	2.112	Oscillator #2 Ckt Failure
105	2 events	DIAMOND	2.109	Oscillator #1 Ckt Failure
		DIAMOND	2.113	Oscillator #2 Frequency Drift
116	2 events	DIAMOND	2.110	Oscillator #1 Frequency Drift
		DIAMOND	2.113	Oscillator #2 Frequency Drift
107	2 events	DIAMOND	2.111	Mixer #1 Failure
		DIAMOND	2.113	Oscillator #2 Frequency Drift

Min Cut Set	Min Cut Set Size	Event Type	Event	Description
108	2 events	DIAMOND	2.109	Oscillator #1 Ckt Failure
		DIAMOND	2.114	Mixer #2 Failure
109	2 events	DIAMOND	2.110	Oscillator #1 Frequency Drift
		DIAMOND	2.114	Mixer #2 Failure
110	2 events	DIAMOND	2.111	Mixer #1 Failure
		DIAMOND	2.114	Mixer #2 Failure
111	2 events	DIAMOND	2.39	LNA #1 Component Failure
		DIAMOND	2.41	LNA #2 Component Failure
112	2 events	DIAMOND	2.40	Loss of Raw Bus Power to LNA #1
		DIAMOND	2.41	LNA #2 Component Failure
113	2 events	DIAMOND	2.39	LNA #1 Component Failure
		DIAMOND	2.42	Loss of Raw Bus Power to LNA #2
114	2 events	DIAMOND	2.40	Loss of Raw Bus Power to LNA #1
		DIAMOND	2.42	Loss of Raw Bus Power to LNA #2

Table B.2 RF Subsystem Minimum Cut Sets

APPENDIX C. DIGITAL CONTROL SUBSYSTEM

FAULT TREE ANALYSIS

This appendix contains the raw data for the FTA of the DCS. Figure C.1 is a functional block diagram of the DCS. The DCS failure end events are listed in Table C.1 and the DCS minimum cut sets generated by the FaultrEASE software program for the PANSAT fault tree in Appendix D are listed in Table C.2.

The minimum cut sets were generated using a direct evaluation technique employed by the software package. The basic end events were compared by their description label contents. There are repeated events listed for this fault tree, but each event is assumed to be different from the rest. This difference, however, may only be in the failure of conductivity between two points. For example, events 3.17 and 3.23 are both microprocessor (μP) failures. The difference between the two events may be two different kinds of μ P failures which could cause different failure paths.

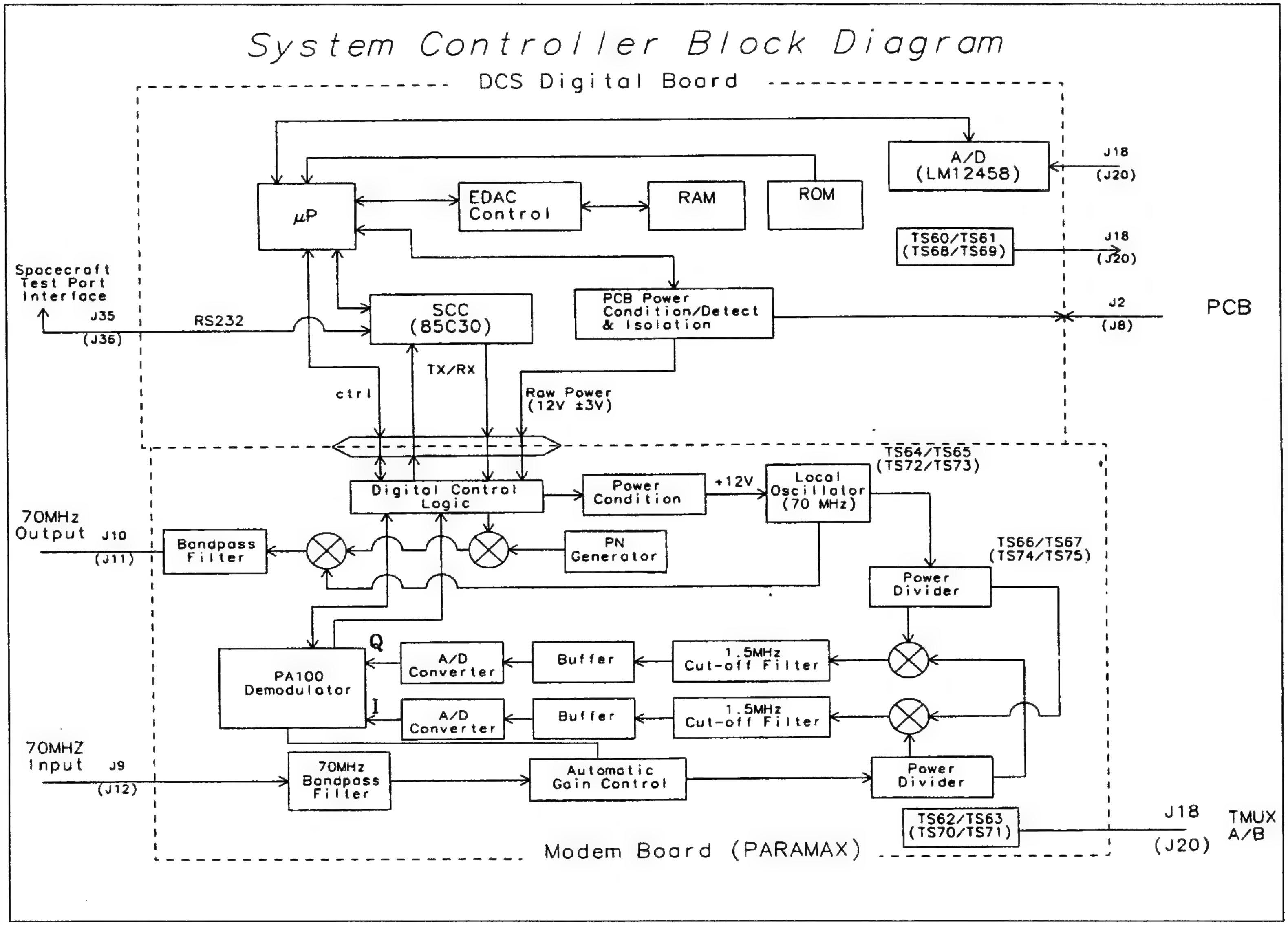


Figure C.1 DCS Block Diagram

Event	End Event Failure	Notes
3.1	MASS A Failure	Contains 4 Mbytes static RAM and 512 Kbytes of flash memory. Accessible from either DCS.
3.2	MASS B Failure	Contains 4 Mbytes static RAM and 512 Kbytes of flash memory. Accessible from either DCS.
3.3	DCS A Interface Ckt (PCB) Failure	Regulates power from raw power bus for the DCS ckt.
3.4	DCS A uP Failure	Commanding and processing unit for the spacecraft
3.5	DCS A EDAC Failure	Failure may cause inability to read from RAM or incorrect data transfer.
3.6	DCS A uP RAM Failure	Limits or prevents uP operations
3.7	DCS A uP ROM Failure	Failure cause inability to load base operating system
3.8	PCB Failure to DCS A	PCB Interface ckt failure
3.9	Peripheral Function	All peripheral sub-system functioning
3.10	Digital Control Ckt Failure	Logic conductivity between uP and SCC to the modem board
3.11	Loss of Raw Bus Power from PCB to DCS A	No power for DCS
3.12	PCB Interface Failure to DCS A	Unable to communicate with peripheral subsystems and/or loss of power for DCS
3.13	DCS A SC Logic Board Power Conditioner Failure	Loss of regulated power for DCS
3.14	DCS A Local Oscillator (70 MHz) Failure	Freq. modulation to/from IF
3.15	DCS A Transmitter Mixer Failure	Failure result in inability to frequency shift transmission data from baseband to IF
3.16	DCS A 70 MHz Transmitter Output Band Pass Filter (BPF)	Failure could reject, distort, or attenuate transmission data stream to RF subsystem.
3.17	DCS A uP Failure	see 3.4
3.18	DCS A EDAC Failure	see 3.5
3.19	DCS A uP RAM Failure	see 3.6
3.20	DCS A uP ROM Failure	see 3.7
3.21	DCS A PA 100	Failure prevents demodulation of received message

Event	End Event Failure	Notes
	PARAMAX Failure	information
3.22	DCS A SCC Failure	Failure prevents message data communication between the uP and modem board
3.23	DCS A uP Failure	see 3.4
3.24	Message Signal from RF Subsystem to DCS A	This is a normal event, not a failure event.
3.25	DCS A In-phase 1.5 MHz Cut-off Freq. Filter Failure	In-phase Bandpass Filter (base band)
3.26	DCS A In-phase Signal Buffer Failure	Buffers incoming bit stream for in-phase signal. Failure could prevent signal flow or lost data.
3.27	DCS A In-phase A/D Failure	Analog to Digital conversion of received in-phase baseband signal
3.28	DCS A 70 MHz Input Bandpass Filter Failure	Failure could reject, distort, or attenuate the received analog IF data message from RF subsystem
3.29	DCS A Input Automatic Gain Control (AGC) Failure	Failure could prevent signal flow or incorrect PARAMAX demodulation
3.30	DCS A 70 MHz Receiver Local Oscillator	Failure would prevent frequency downshift from IF to baseband.
3.31	DCS A Power Divider Failure	Failure could prevent local oscillator signal to mixer, therefore no frequency downshift
3.32	DCS A Quad Ckt Input Mixer Failure	Failure would prevent frequency downshift to baseband for quadrature phase signal
3.33	DCS A In-phase Ckt Input Mixer Failure	Failure would prevent in-phase message demodulation.
3.34	DCS A Receiver Input Signal Power Divider	see 3.31
3.35	DCS A Quad. 1.5 MHz Cut-off Freq. Filter Failure	Quadrature phase Bandpass Filter (base band)
3.36	DCS A Quad. Signal Buffer Failure	Buffers incoming bit stream for quadrature signal. Failure could prevent signal flow or lost data.
3.37	DCS A Quad. A/D Failure	Analog to Digital conversion of received quadrature phase baseband signal

Event	End Event Failure	Notes
3.38	DCS B Interface Ckt (PCB) Failure	Same as for DCS A above
3.39	DCS B uP Failure	Same as for DCS A above
3.40	DCS B EDAC Failure	Same as for DCS A above
3.41	DCS B uP RAM Failure	Same as for DCS A above
3.42	DCS B uP ROM Failure	Same as for DCS A above
3.43	PCB Failure to DCS B	Same as for DCS A above
3.44	DCS B Digital Control Ckt Failure	Same as for DCS A above
3.45	Loss of Raw Bus Power from PCB to DCS B	Same as for DCS A above
3.46	PCB Interface Failure to DCS B	Same as for DCS A above
3.47	DCS B Logic Board Power Conditioner Failure	Same as for DCS A above
3.48	DCS B Local Oscillator (70 MHz) Failure	Same as for DCS A above
3.49	DCS B Transmitter Mixer Failure	Same as for DCS A above
3.50	DCS B 70 MHz Transmitter Output Band Pass Filter (BPF)	Same as for DCS A above
3.51	DCS B uP Failure	Same as for DCS A above
3.52	DCS B EDAC Failure	Same as for DCS A above
3.53	DCS B uP RAM Failure	Same as for DCS A above
3.54	DCS B uP ROM Failure	Same as for DCS A above
3.55	DCS B PA 100 PARAMAX Failure	Same as for DCS A above
3.56	DCS B SCC Failure	Same as for DCS A above
3.57	DCS B uP Failure	Same as for DCS A above
3.58	Message Signal from RF Subsystem to DCS B	Same as for DCS A above
3.59	DCS B In-phase 1.5 MHz	Same as for DCS A above

Event	End Event Failure	Notes
	Cut-off Freq. Filter Failure	
3.60	DCS B In-phase Signal Buffer Failure	Same as for DCS A above
3.61	DCS B In-phase A/D Failure	Same as for DCS A above
3.62	DCS B 70 MHz Input Bandpass Filter Failure	Same as for DCS A above
3.63	DCS B Input Automatic Gain Control (AGC) Failure	Same as for DCS A above
3.64	DCS B 70 MHz Receiver Local Oscillator	Same as for DCS A above
3.65	DCS B Power Divider Failure	Same as for DCS A above
3.66	DCS B Quad Ckt Input Mixer Failure	Same as for DCS A above
3.67	DCS B In-phase Ckt Input Mixer Failure	Same as for DCS A above
3.68	DCS B Receiver Input Signal Power Divider	Same as for DCS A above
3.69	DCS B Quad. 1.5 MHz Cut-off Freq. Filter Failure	Same as for DCS A above
3.70	DCS B Quad. Signal Buffer Failure	Same as for DCS A above
3.71	DCS B Quad. A/D Failure	Same as for DCS A above

Table C.1 Digital Control System Critical Failure Events

Min Cut Set	Min. Cut Set Size	Event Type	Event	Description
1	1 event	DIAMOND	3.3	DCS A Interface Ckt (PCB) Failure
2	1 event	DIAMOND	3.4	DCS A uP Failure
3	1 event	DIAMOND	3.5	DCS A EDAC Failure
4	1 event	DIAMOND	3.6	DCS A uP RAM Failure
5	1 event	DIAMOND	3.7	DCS A uP ROM Failure
6	1 event	DIAMOND	3.8	PCB Failure to DCS A
7	1 event	DIAMOND	3.10	DCS A Digital Control Ckt Failure
8	1 event	DIAMOND	3.11	Loss of Raw Bus Power from PCB to DCS A
9	1 event	DIAMOND	3.12	PCB Interface Failure to DCS A
10	1 event	DIAMOND	3.13	DCS A SC Logic Board Power Conditioner Failure
11	1 event	DIAMOND	3.14	DCS A Local Oscillator (70 MHz) Failure
12	1 event	DIAMOND	3.15	DCS A Transmitter Mixer Failure
13	1 event	DIAMOND	3.16	DCS A 70 MHz Transmitter Output Band Pass Filter (BPF)
14	1 event	DIAMOND	3.21	DCS A PA 100 PARAMAX Failure
15	1 event	DIAMOND	3.22	DCS A SCC Failure
16	1 event	DIAMOND	3.25	DCS A In-phase 1.5 MHz Cut-off Freq. Filter Failure
17	1 event	DIAMOND	3.26	DCS A In-phase Signal Buffer Failure
18	1 event	DIAMOND	3.27	DCS A In-phase A/D Failure
19	1 event	DIAMOND	3.28	DCS A 70 MHz Input Bandpass Filter Failure
20	1 event	DIAMOND	3.29	DCS A Input Automatic Gain Control (AGC) Failure
21	1 event	CIRCLE	3.31	DCS A Power Divider Failure
22	1 event	CIRCLE	3.32	DCS A Quad Ckt Input Mixer Failure
23	1 event	CIRCLE	3.33	DCS A In-phase Ckt Input Mixer Failure
24	1 event	CIRCLE	3.34	DCS A Receiver Input Signal Power Divider
25	1 event	DIAMOND	3.35	DCS A Quad. 1.5 MHz Cut-off Freq. Filter Failure

Min Cut Set	Min. Cut Set Size	Event Type	Event	Description
26	1 event	DIAMOND	3.36	DCS A Quad. Signal Buffer Failure
27	1 event	DIAMOND	3.37	DCS A Quad. A/D Failure
28	1 event	DIAMOND	3.38	DCS B Interface Ckt (PCB) Failure
29	1 event	DIAMOND	3.39	DCS B uP Failure
30	1 event	DIAMOND	3.40	0DCS B EDAC Failure
31	1 event	DIAMOND	3.41	DCS B uP RAM Failure
32	1 event	DIAMOND	3.42	DCS B uP ROM Failure
33	1 event	DIAMOND	3.43	PCB Failure to DCS B
34	1 event	DIAMOND	3.44	DCS B Digital Control Ckt Failure
35	1 event	DIAMOND	3.45	Loss of Raw Bus Power from PCB to DCS B
36	1 event	DIAMOND	3.46	PCB Interface Failure to DCS B
37	1 event	DIAMOND	3.47	DSC B Logic Board Power Conditioner Failure
38	1 event	DIAMOND	3.48	DCS B Local Oscillator (70 MHz) Failure
39	1 event	DIAMOND	3.49	DCS B Transmitter Mixer Failure
40	1 event	DIAMOND	3.50	DCS B 70 MHz Transmitter Output Band Pass Filter (BPF)
41	1 event	DIAMOND	3.55	DCS B PA 100 PARAMAX Failure
42	1 event	DIAMOND	3.56	DCS B SCC Failure
43	1 event	DIAMOND	3.59	DCS B In-phase 1.5 MHz Cut-off Freq. Filter Failure
44	1 event	DIAMOND	3.60	DCS B In-phase Signal Buffer Failure
45	1 event	DIAMOND	3.61	DCS B In-phase A/D Failure
46	1 event	DIAMOND	3.62	DCS B 70 MHz Input Bandpass Filter Failure
47	1 event	DIAMOND	3.63	DCS B Input Automatic Gain Control (AGC) Failure
48	1 event	CIRCLE	3.65	DCS B Power Divider Failure
49	1 event	CIRCLE	3.66	DCS B Quad Ckt Input Mixer Failure
50	1 event	CIRCLE	3.67	DCS B In-phase Ckt Input Mixer Failure
51	1 event	CIRCLE	3.68	DCS B Receiver Input Signal Power Divider

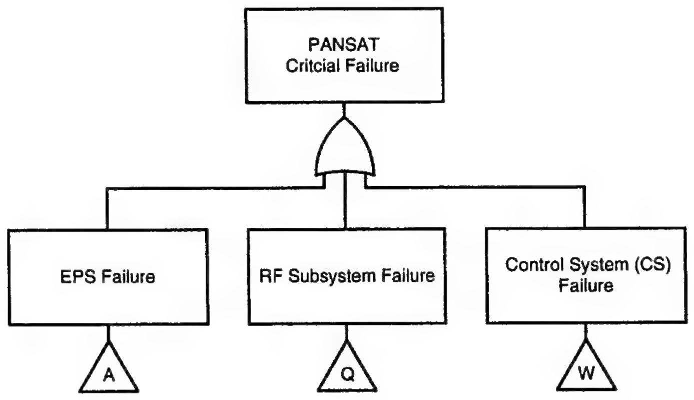
Min Cut Set	Min. Cut Set Size	Event Type	Event	Description
52	1 event	DIAMOND	3.69	DCS B Quad. 1.5 MHz Cut-off Freq. Filter Failure
53	1 event	DIAMOND	3.70	DCS B Quad. Signal Buffer Failure
54	1 event	DIAMOND	3.71	DCS B Quad. A/D Failure
55	2 events	DIAMOND	3.2	MASS B Failure
		DIAMOND	3.1	MASS A Failure

Table C.2 DCS Minimum Cut Sets

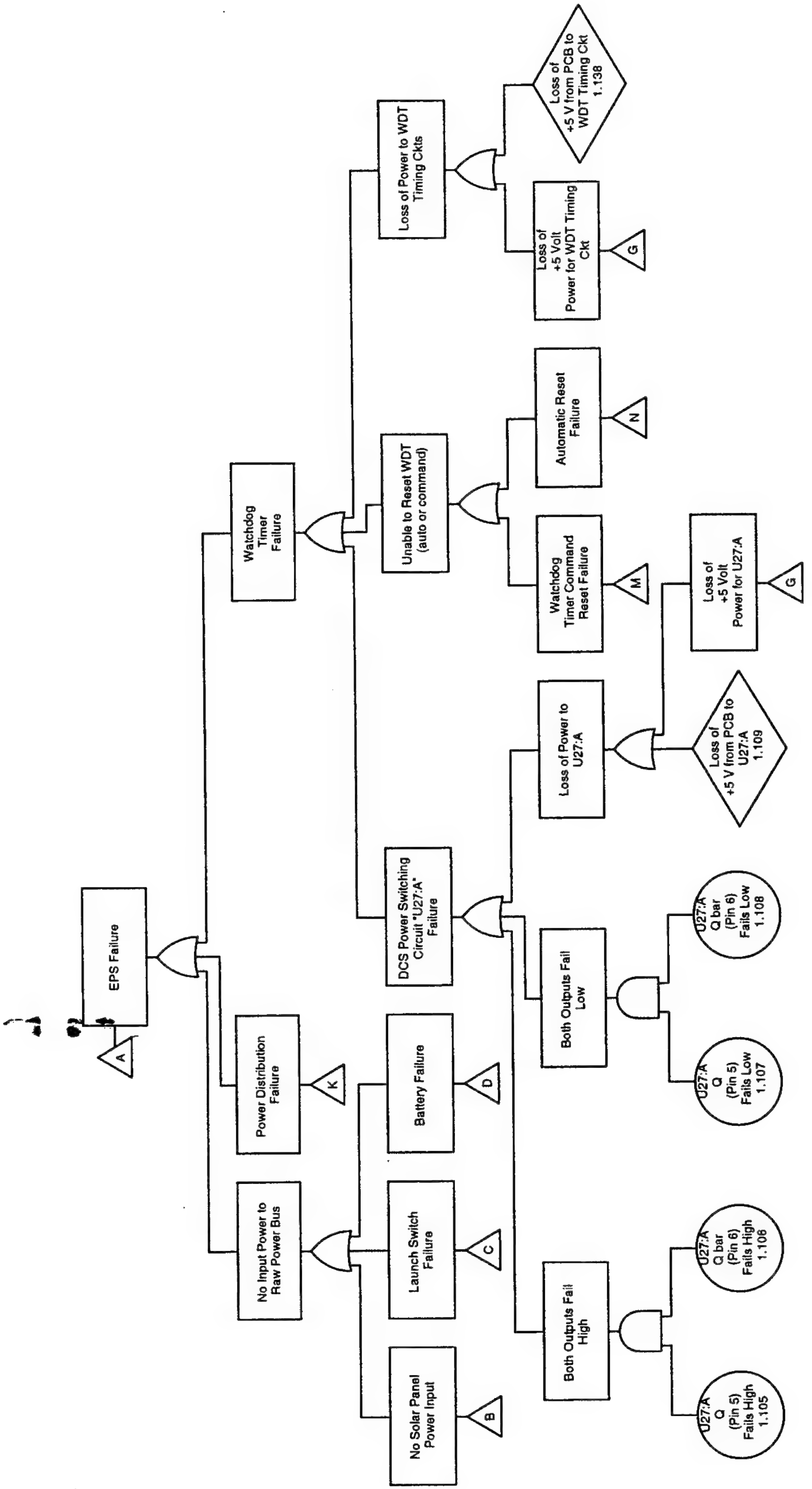
APPENDIX D. PANSAT FAULT TREE

This appendix contains the PANSAT fault tree constructed using the FaultrEASE software program. The small triangle end events (called transfers) denote the continuation of the fault tree on a following page. The letter inside the transfer symbol logically link the pages.

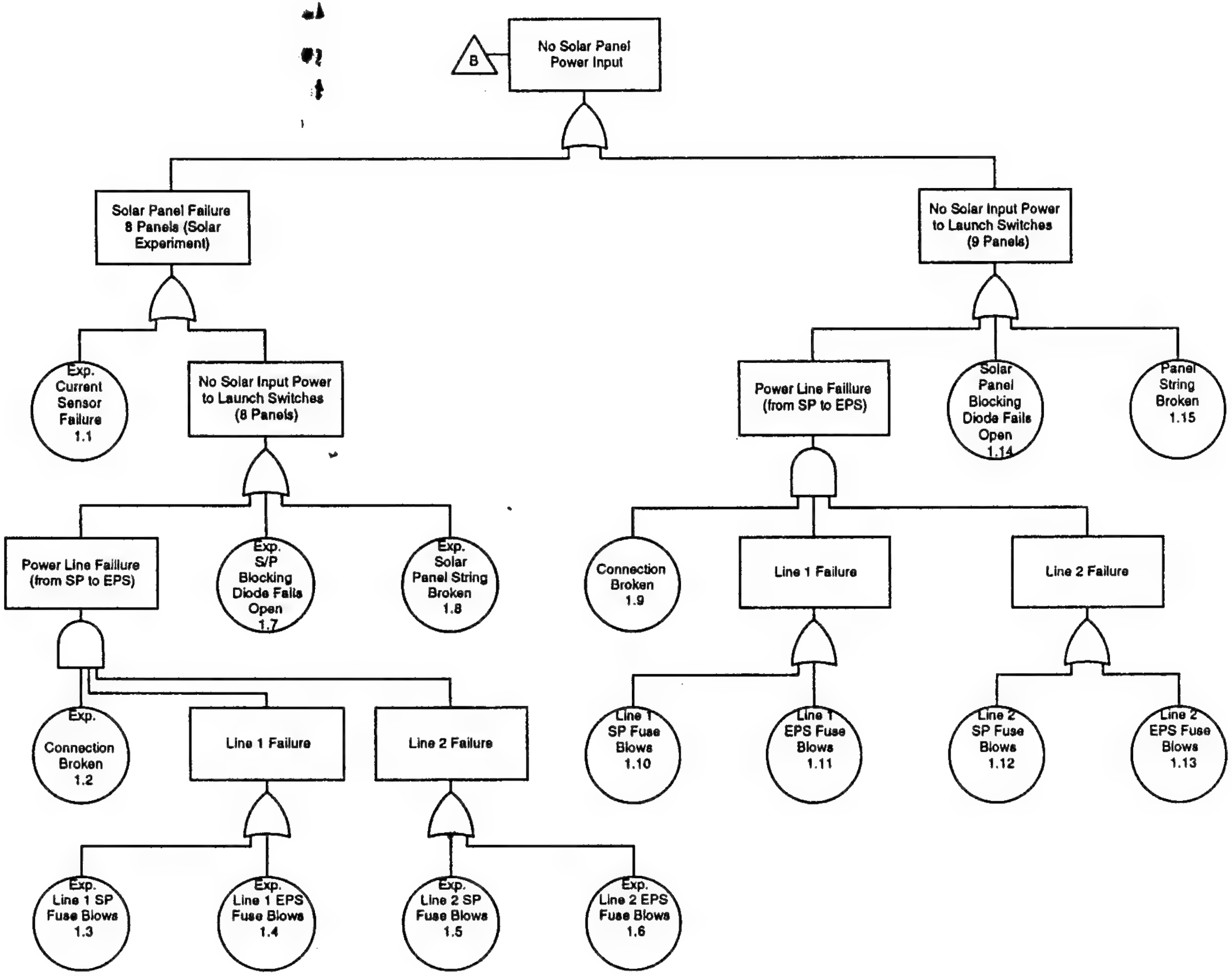
PANSAT CRITICAL FAILURE



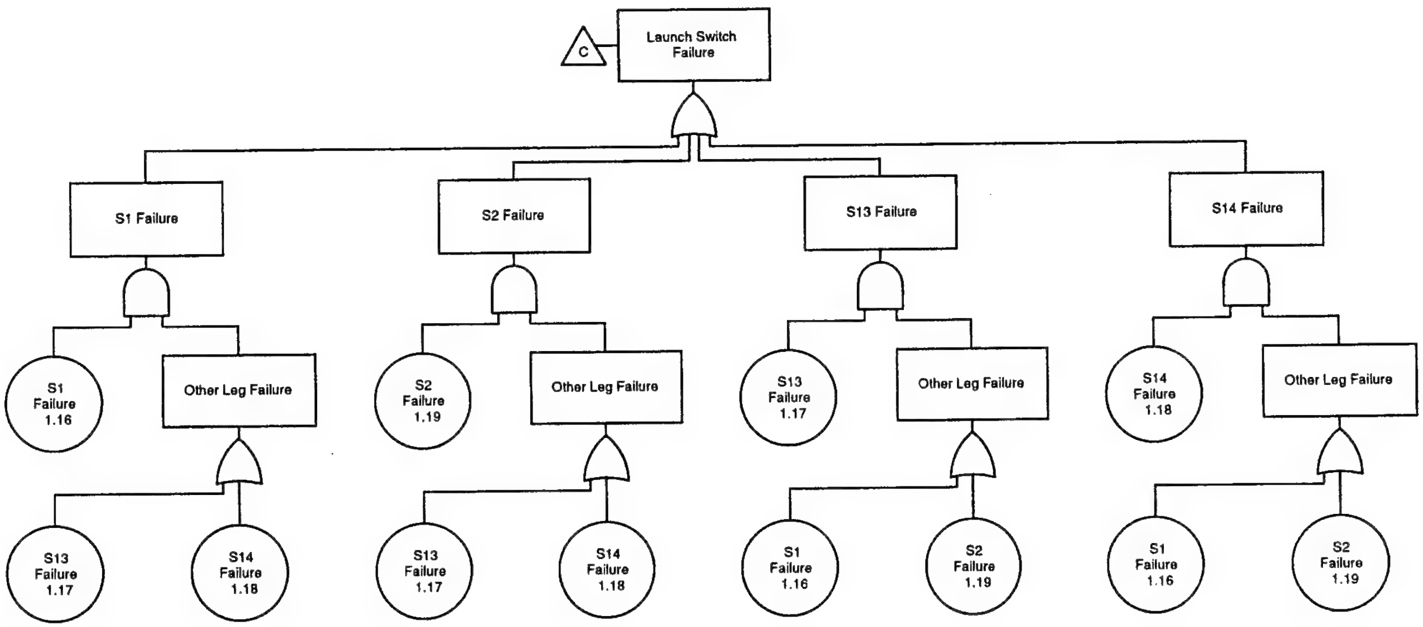
Electrical Power Subsystem (EPS)


EPS Failure
A
Watchdog Timer Failure
Power Distribution Failure
K
No Input Power to Raw Power Bus
No Solar Panel Power Input
B
Launch Switch Failure
C
Battery Failure
D
DCS Power Switching Circuit "U27:A" Failure
Unable to Reset WDT (auto or command)
Loss of Power to WDT Timing Ckts
Loss of +5 Volt Power for WDT Timing Ckt
G
Loss of +5 V from PCB to WDT Timing Ckt 1.138
Automatic Reset Failure
N
Watchdog Timer Command Reset Failure
M
Loss of Power to U27:A
Loss of +5 Volt Power for U27:A
G
Loss of +5 V from PCB to U27:A 1.109
Both Outputs Fail Low
U27:A Q bar (Pin 6) Fails Low 1.108
U27:A Q (Pin 5) Fails Low 1.107
Both Outputs Fail High
U27:A Q bar (Pin 6) Fails High 1.106
U27:A Q (Pin 5) Fails High 1.105

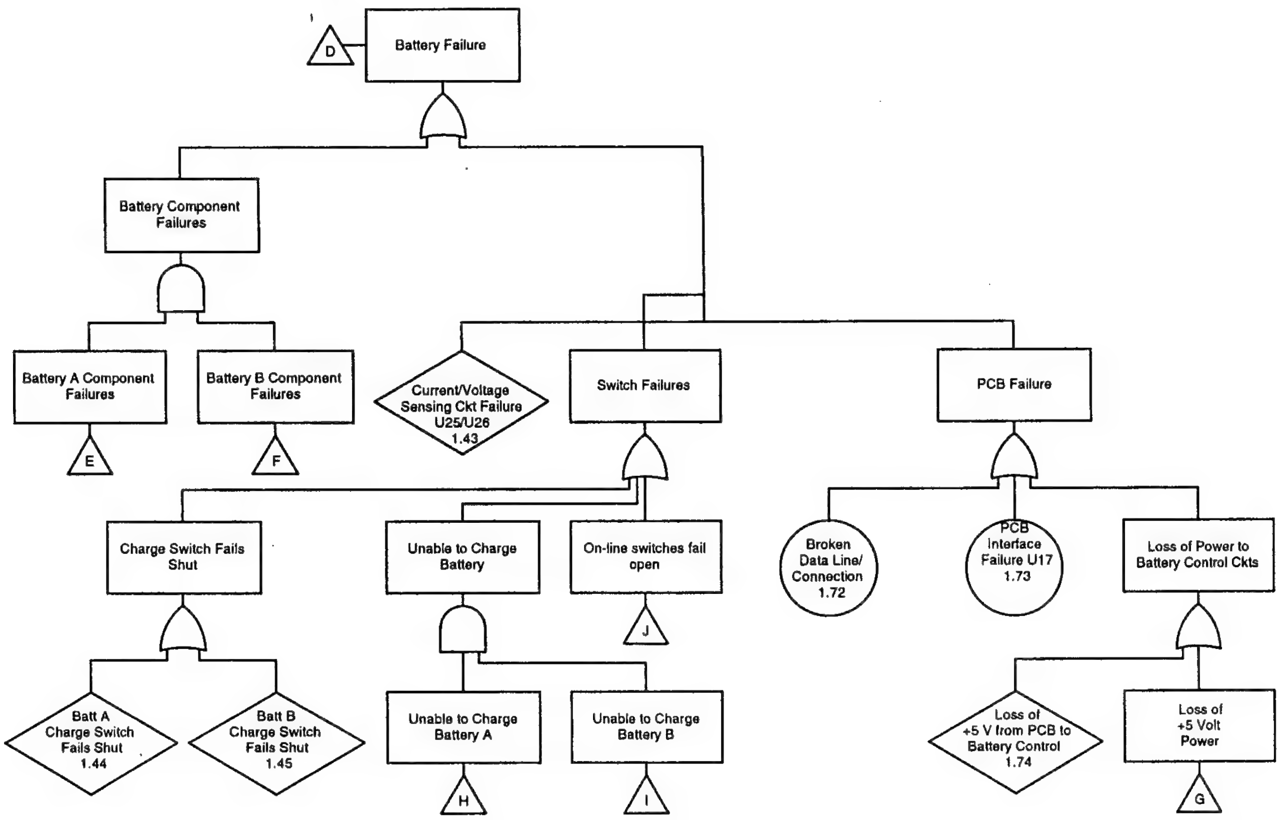
SOLAR PANEL FAILURE


B
No Solar Panel Power Input
Solar Panel Failure 8 Panels (Solar Experiment)
No Solar Input Power to Launch Switches (9 Panels)
Exp. Current Sensor Failure 1.1
No Solar Input Power to Launch Switches (8 Panels)
Power Line Faillure (from SP to EPS)
Solar Panel Blocking Diode Fails Open 1.14
Panel String Broken 1.15
Power Line Faillure (from SP to EPS)
Exp. S/P Blocking Diode Fails Open 1.7
Exp. Solar Panel String Broken 1.8
Connection Broken 1.9
Line 1 Failure
Line 2 Failure
Exp. Connection Broken 1.2
Line 1 Failure
Line 2 Failure
Line 1 SP Fuse Blows 1.10
Line 1 EPS Fuse Blows 1.11
Line 2 SP Fuse Blows 1.12
Line 2 EPS Fuse Blows 1.13
Exp. Line 1 SP Fuse Blows 1.3
Exp. Line 1 EPS Fuse Blows 1.4
Exp. Line 2 SP Fuse Blows 1.5
Exp. Line 2 EPS Fuse Blows 1.6

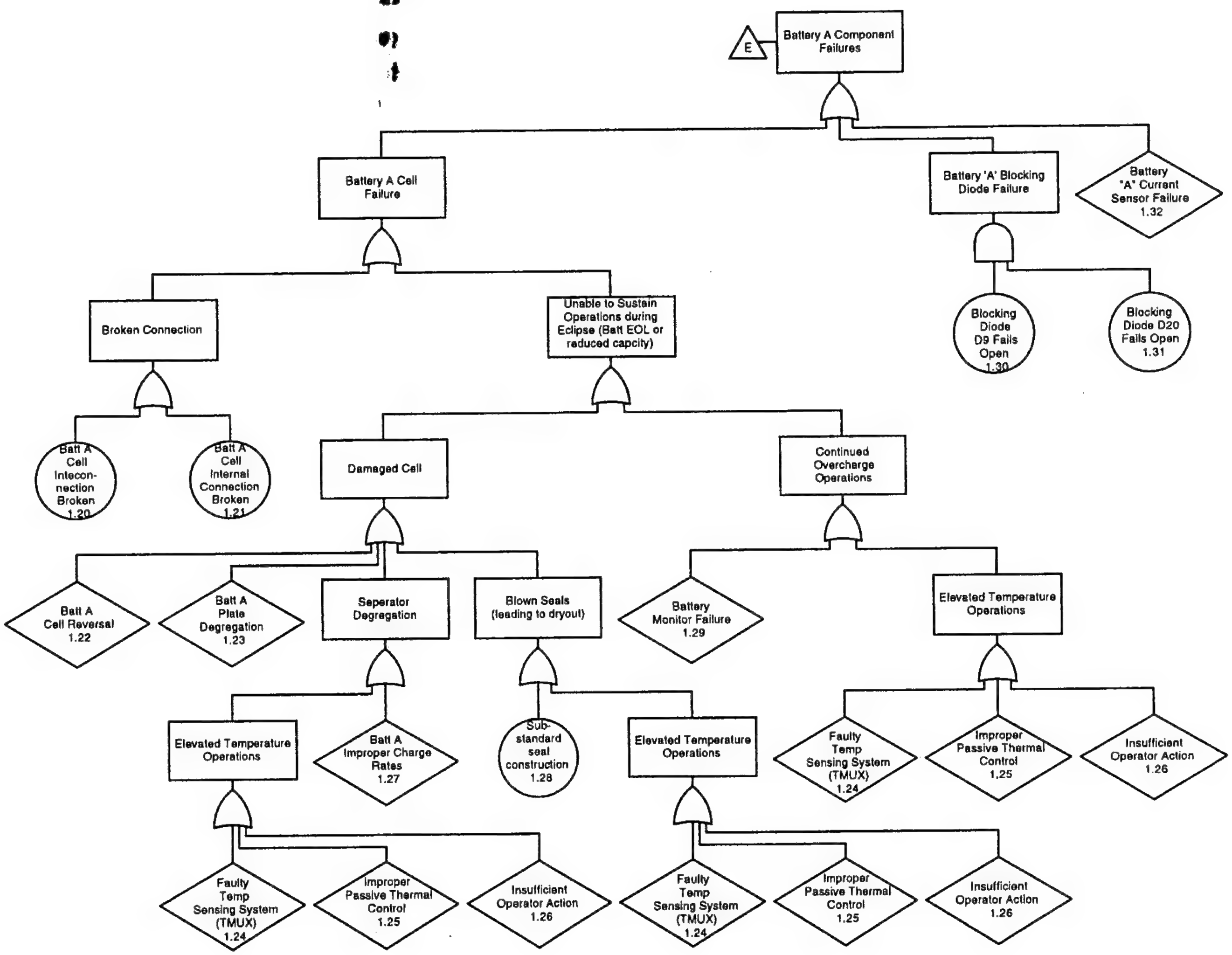
LAUNCH SWITCH FAILURE



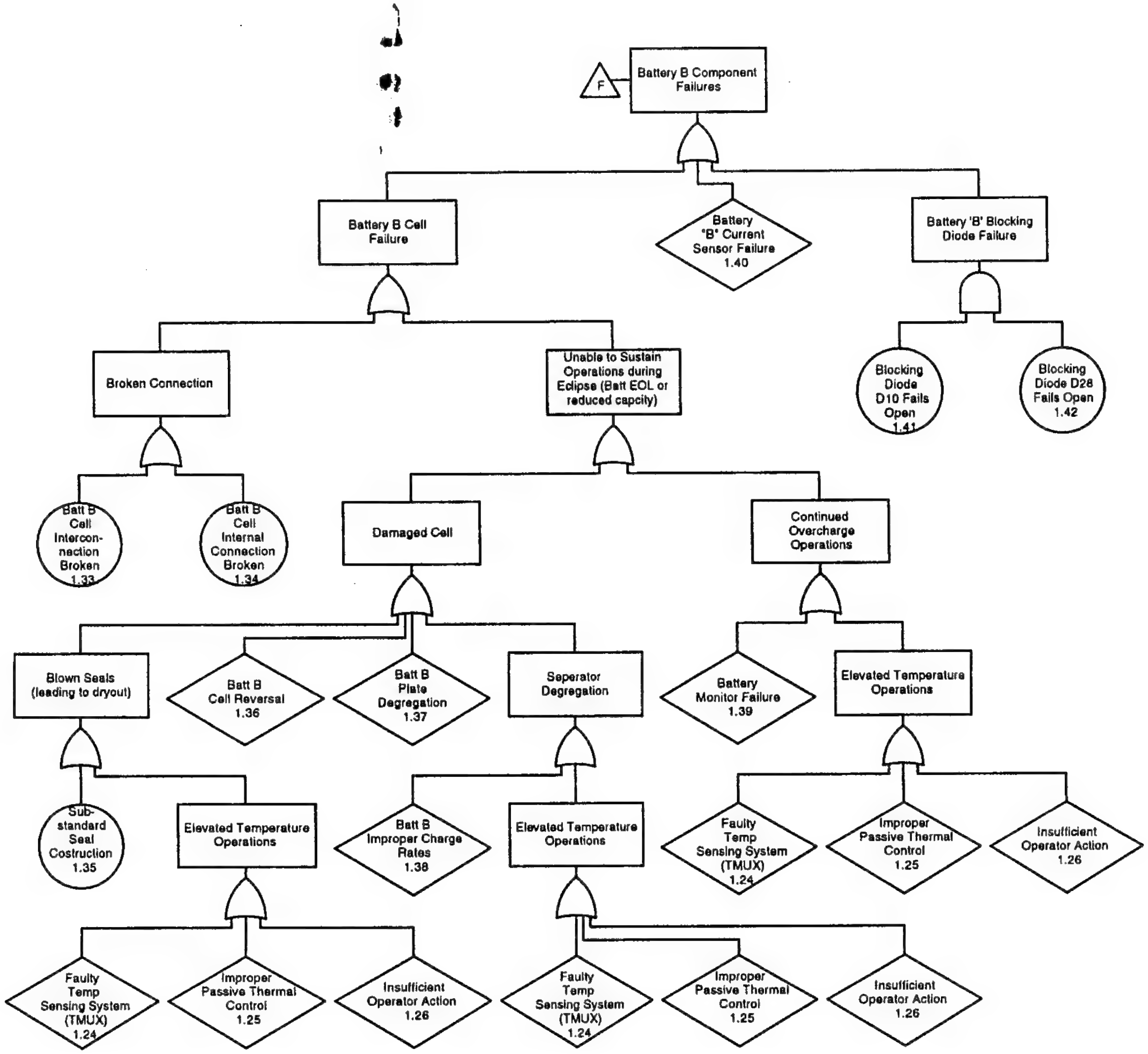
STORAGE BATTERY FAILURE


D
Battery Failure
Battery Component Failures
Battery A Component Failures
E
Battery B Component Failures
F
Current/Voltage Sensing Ckt Failure U25/U26 1.43
Switch Failures
PCB Failure
Charge Switch Fails Shut
Batt A Charge Switch Fails Shut 1.44
Batt B Charge Switch Fails Shut 1.45
Unable to Charge Battery
Unable to Charge Battery A
H
Unable to Charge Battery B
I
On-line switches fail open
J
Broken Data Line/ Connection 1.72
PCB Interface Failure U17 1.73
Loss of Power to Battery Control Ckts
Loss of +5 V from PCB to Battery Control 1.74
Loss of +5 Volt Power
G

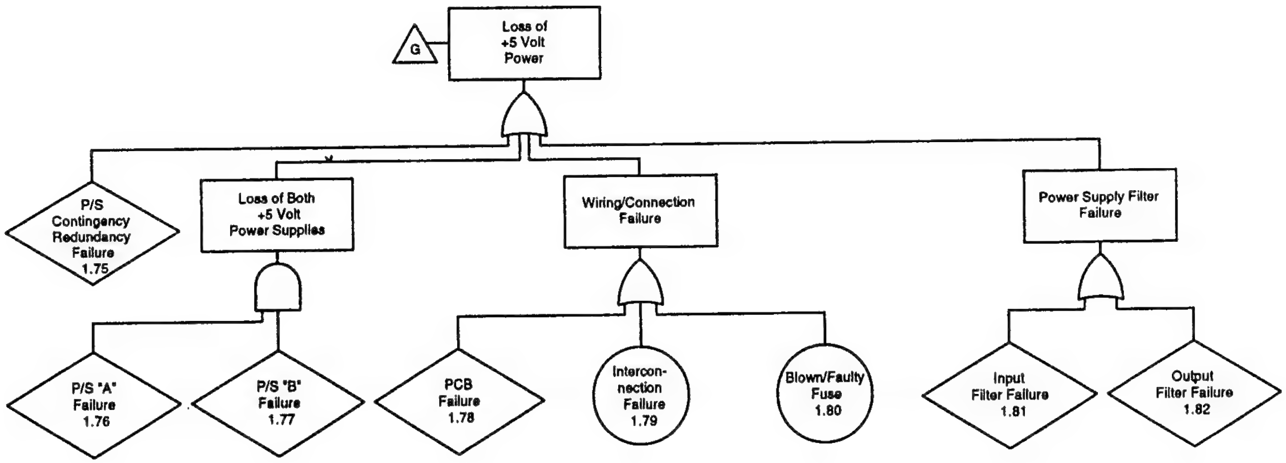
BATTERY A COMPONENT FAILURE


E
Battery A Component Failures
Battery A Cell Failure
Battery 'A' Blocking Diode Failure
Battery "A" Current Sensor Failure 1.32
Blocking Diode D9 Fails Open 1.30
Blocking Diode D20 Fails Open 1.31
Broken Connection
Unable to Sustain Operations during Eclipse (Batt EOL or reduced capcity)
Batt A Cell Intecon-nection Broken 1.20
Batt A Cell Internal Connection Broken 1.21
Damaged Cell
Continued Overcharge Operations
Batt A Cell Reversal 1.22
Batt A Plate Degregation 1.23
Seperator Degregation
Blown Seals (leading to dryout)
Battery Monitor Failure 1.29
Elevated Temperature Operations
Elevated Temperature Operations
Batt A Improper Charge Rates 1.27
Sub-standard seal construction 1.28
Elevated Temperature Operations
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26

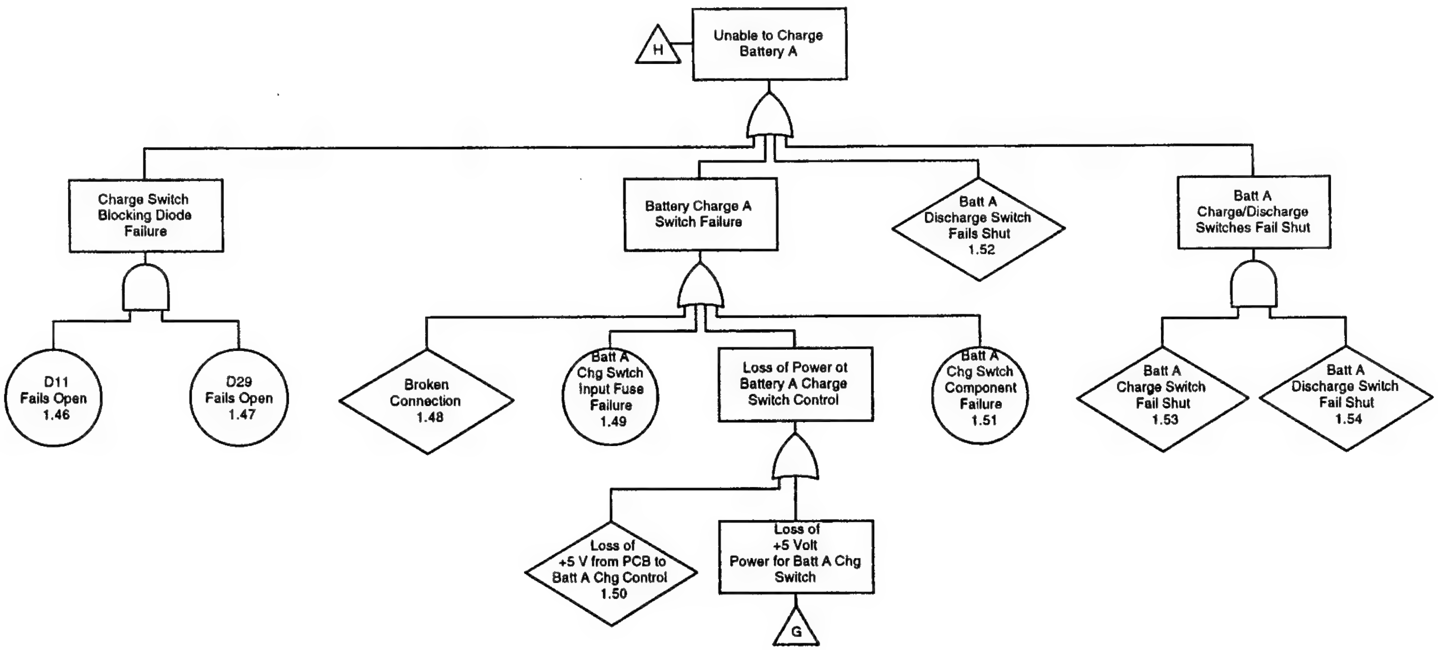
BATTERY B COMPONENT FAILURE


F
Battery B Component Failures
Battery B Cell Failure
Battery "B" Current Sensor Failure 1.40
Battery 'B' Blocking Diode Failure
Blocking Diode D10 Fails Open 1.41
Blocking Diode D28 Fails Open 1.42
Broken Connection
Unable to Sustain Operations during Eclipse (Batt EOL or reduced capcity)
Batt B Cell Intercon-nection Broken 1.33
Batt B Cell Internal Connection Broken 1.34
Damaged Cell
Continued Overcharge Operations
Blown Seals (leading to dryout)
Batt B Cell Reversal 1.36
Batt B Plate Degregation 1.37
Seperator Degregation
Battery Monitor Failure 1.39
Elevated Temperature Operations
Sub-standard Seal Costruction 1.35
Elevated Temperature Operations
Batt B Improper Charge Rates 1.38
Elevated Temperature Operations
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26
Faulty Temp Sensing System (TMUX) 1.24
Improper Passive Thermal Control 1.25
Insufficient Operator Action 1.26

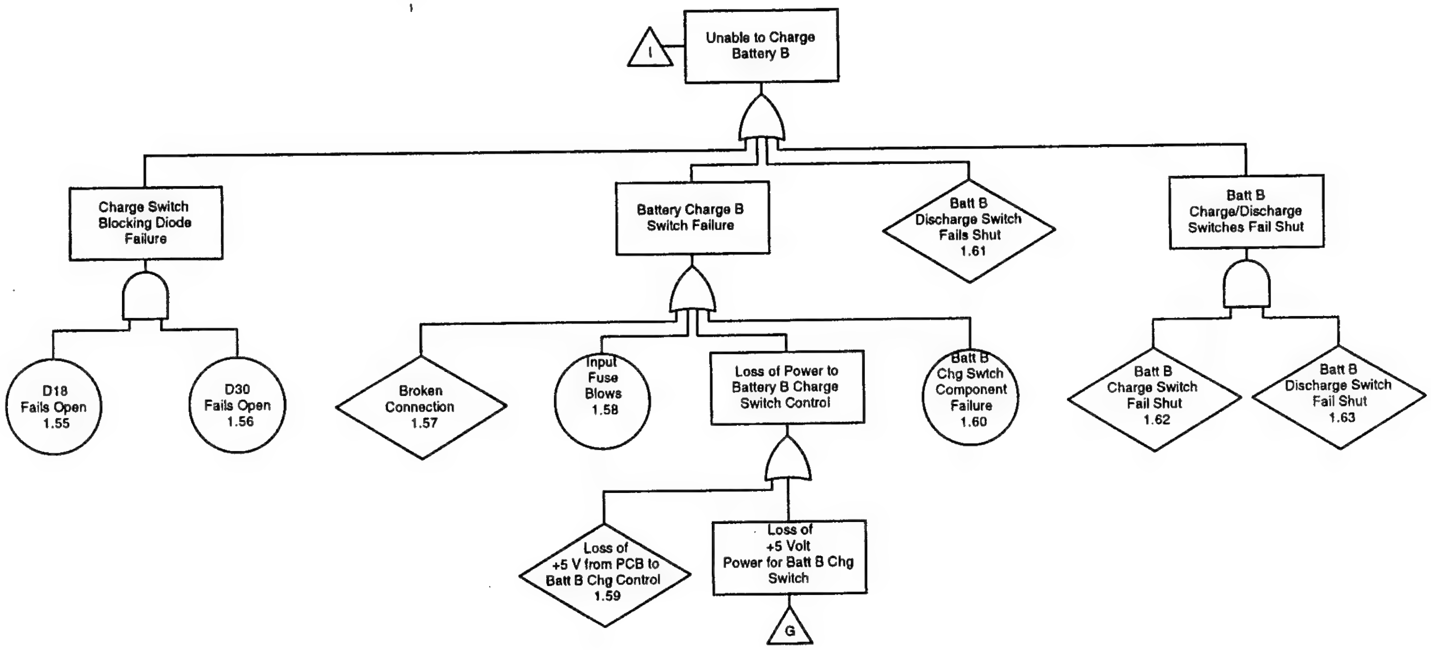
+5 VOLT DUAL POWER SUPPLY FAILURE


G
Loss of +5 Volt Power
P/S Contingency Redundancy Failure 1.75
Loss of Both +5 Volt Power Supplies
Wiring/Connection Failure
Power Supply Filter Failure
P/S "A" Failure 1.76
P/S "B" Failure 1.77
PCB Failure 1.78
Intercon-nection Failure 1.79
Blown/Faulty Fuse 1.80
Input Filter Failure 1.81
Output Filter Failure 1.82

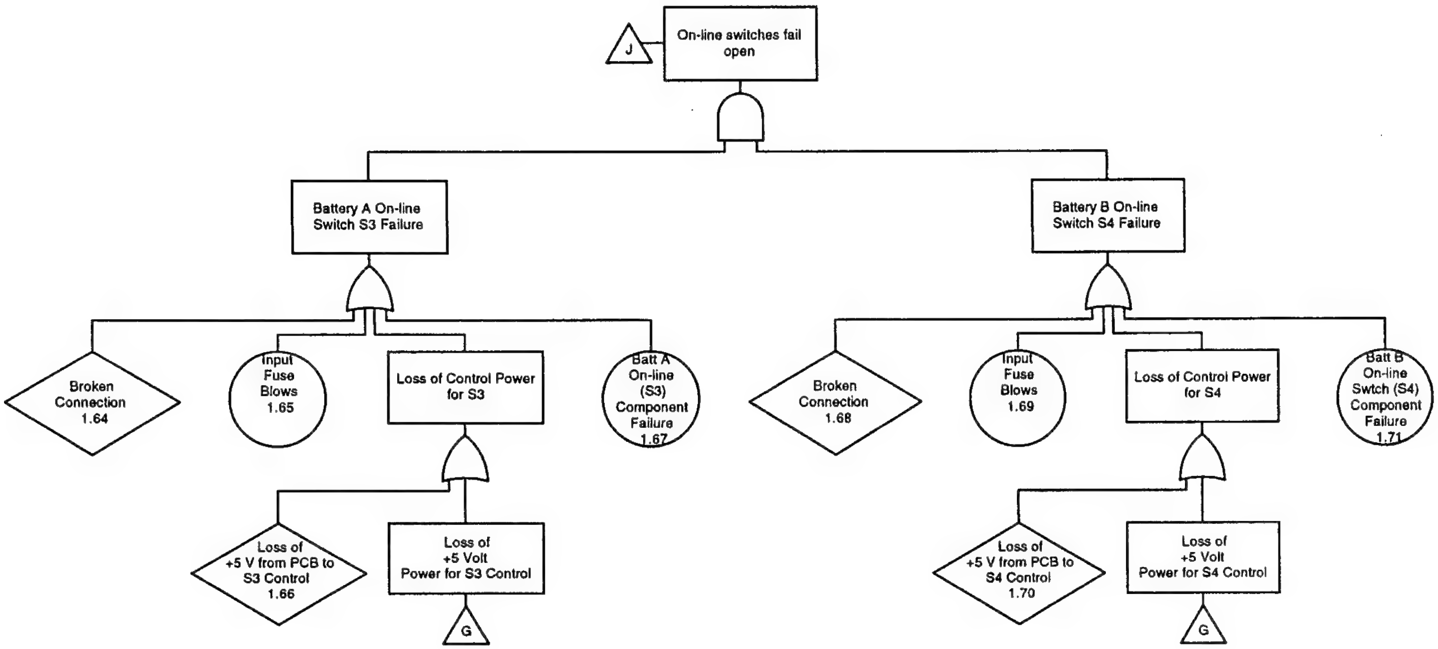
BATTERY A CHARGE SYSTEM FAILURE


H
Unable to Charge Battery A
Charge Switch Blocking Diode Failure
D11 Fails Open 1.46
D29 Fails Open 1.47
Battery Charge A Switch Failure
Broken Connection 1.48
Batt A Chg Swtch Input Fuse Failure 1.49
Loss of Power ot Battery A Charge Switch Control
Loss of +5 V from PCB to Batt A Chg Control 1.50
Loss of +5 Volt Power for Batt A Chg Switch
G
Batt A Chg Swtch Component Failure 1.51
Batt A Discharge Switch Fails Shut 1.52
Batt A Charge/Discharge Switches Fail Shut
Batt A Charge Switch Fail Shut 1.53
Batt A Discharge Switch Fail Shut 1.54

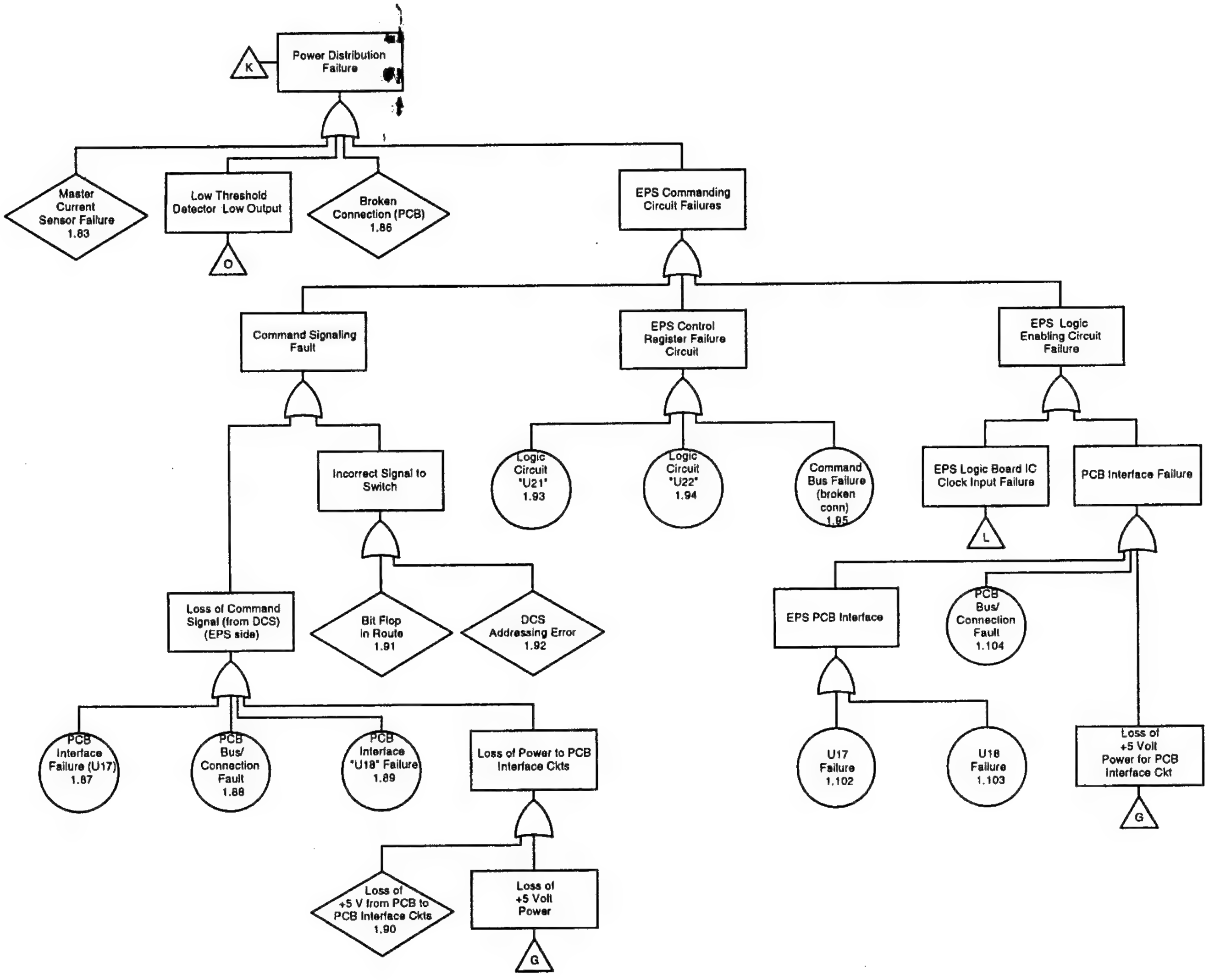
BATTERY B CHARGE SYSTEM FAILURE


I
Unable to Charge Battery B
Charge Switch Blocking Diode Failure
Battery Charge B Switch Failure
Batt B Discharge Switch Fails Shut 1.61
Batt B Charge/Discharge Switches Fail Shut
D18 Fails Open 1.55
D30 Fails Open 1.56
Broken Connection 1.57
Input Fuse Blows 1.58
Loss of Power to Battery B Charge Switch Control
Batt B Chg Swtch Component Failure 1.60
Batt B Charge Switch Fail Shut 1.62
Batt B Discharge Switch Fail Shut 1.63
Loss of +5 V from PCB to Batt B Chg Control 1.59
Loss of +5 Volt Power for Batt B Chg Switch
G

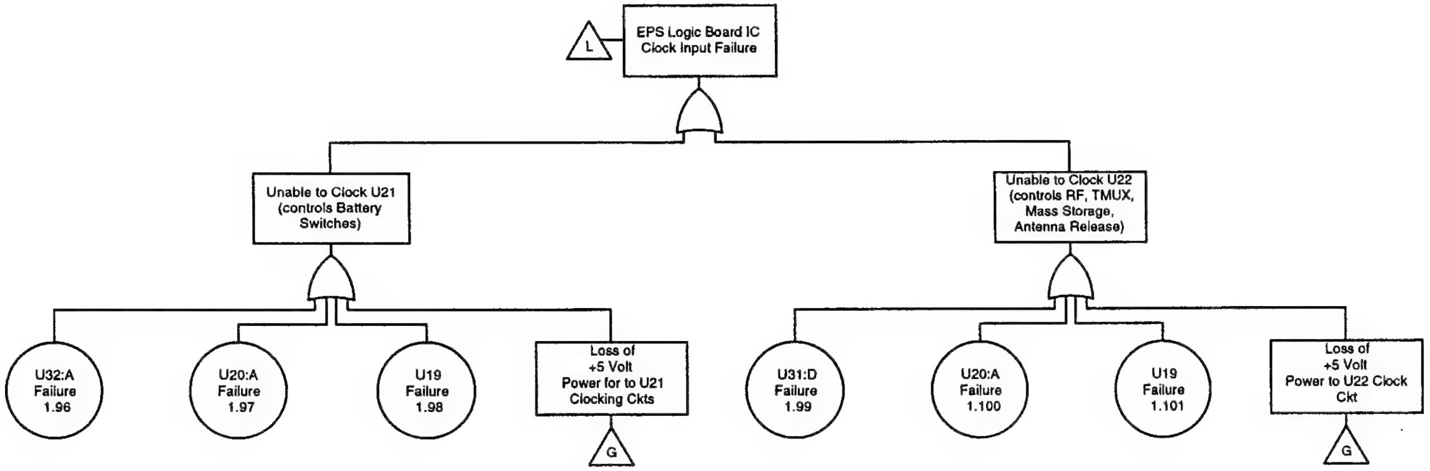
BATTERY ON-LINE SWITCH FAILURE


J
On-line switches fail open
Battery A On-line Switch S3 Failure
Battery B On-line Switch S4 Failure
Broken Connection 1.64
Input Fuse Blows 1.65
Loss of Control Power for S3
Batt A On-line (S3) Component Failure 1.67
Loss of +5 V from PCB to S3 Control 1.66
Loss of +5 Volt Power for S3 Control
G
Broken Connection 1.68
Input Fuse Blows 1.69
Loss of Control Power for S4
Batt B On-line Swtch (S4) Component Failure 1.71
Loss of +5 V from PCB to S4 Control 1.70
Loss of +5 Volt Power for S4 Control
G

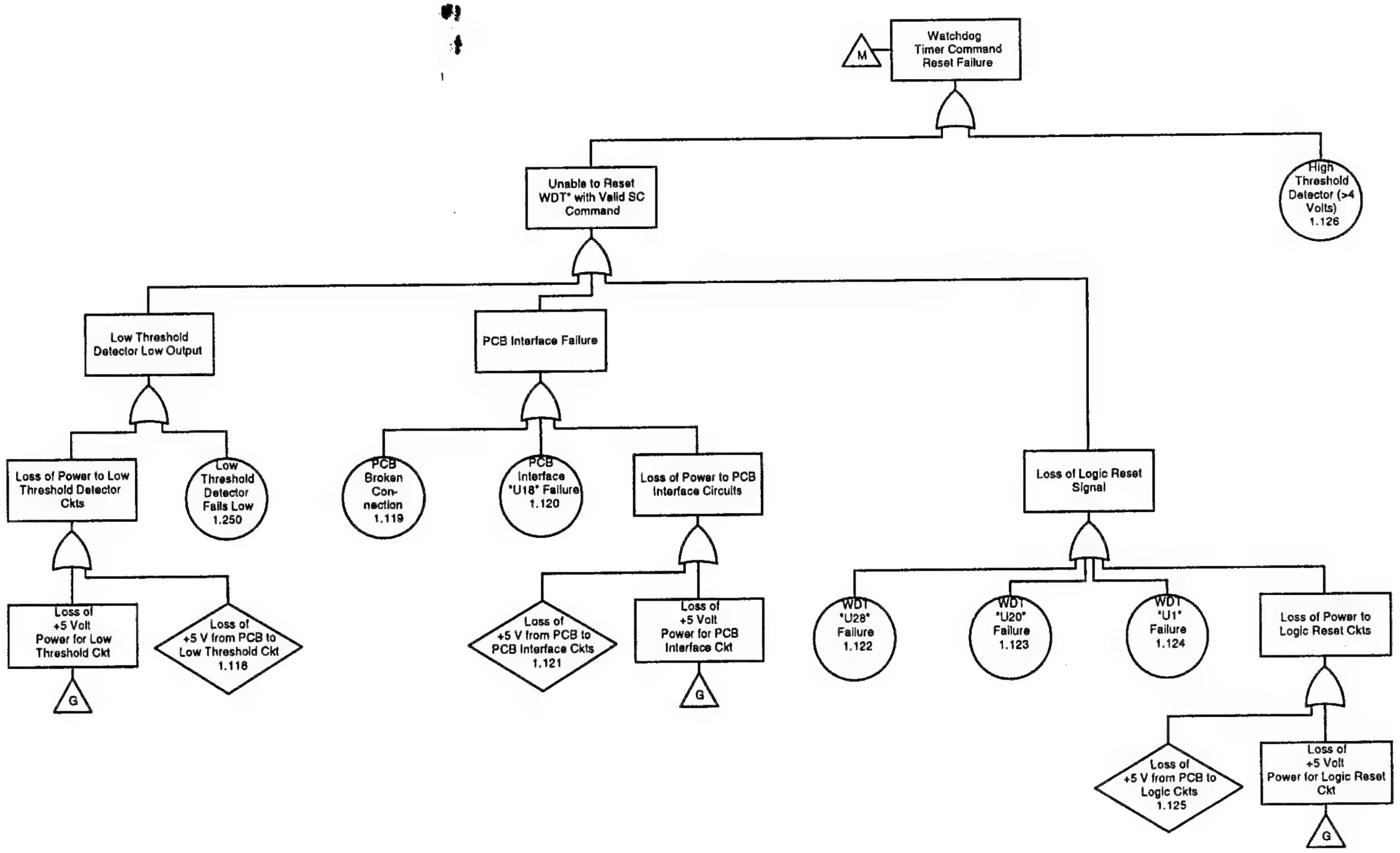
POWER DISTRIBUTION FAILURE


Power Distribution Failure
K
Master Current Sensor Failure 1.83
Low Threshold Detector Low Output
O
Broken Connection (PCB) 1.86
EPS Commanding Circuit Failures
Command Signaling Fault
EPS Control Register Failure Circuit
EPS Logic Enabling Circuit Failure
Incorrect Signal to Switch
Logic Circuit "U21" 1.93
Logic Circuit "U22" 1.94
Command Bus Failure (broken conn) 1.85
EPS Logic Board IC Clock Input Failure
L
PCB Interface Failure
Loss of Command Signal (from DCS) (EPS side)
Bit Flop In Route 1.91
DCS Addressing Error 1.92
EPS PCB Interface
PCB Bus/ Connection Fault 1.104
PCB Interface Failure (U17) 1.87
PCB Bus/ Connection Fault 1.88
PCB Interface "U18" Failure 1.89
Loss of Power to PCB Interface Ckts
U17 Failure 1.102
U18 Failure 1.103
Loss of +5 Volt Power for PCB Interface Ckt
G
Loss of +5 V from PCB to PCB Interface Ckts 1.90
Loss of +5 Volt Power
G

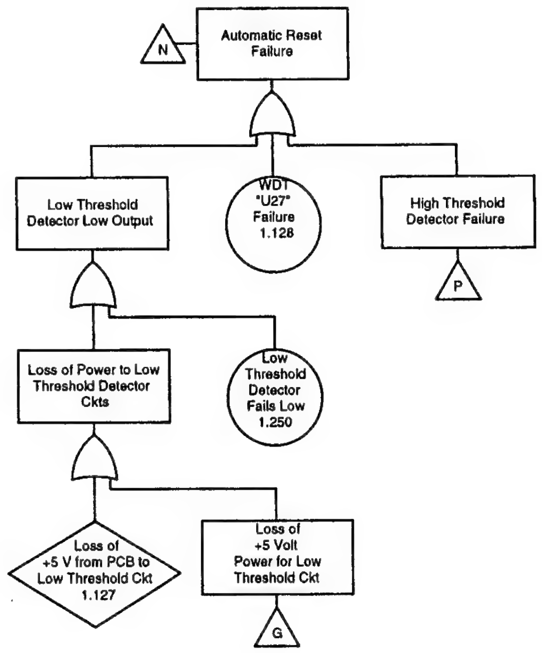
EPS LOGIC BOARD FAILURE


L
EPS Logic Board IC Clock Input Failure
Unable to Clock U21 (controls Battery Switches)
Unable to Clock U22 (controls RF, TMUX, Mass Storage, Antenna Release)
U32:A Failure 1.96
U20:A Failure 1.97
U19 Failure 1.98
Loss of +5 Volt Power for to U21 Clocking Ckts
G
U31:D Failure 1.99
U20:A Failure 1.100
U19 Failure 1.101
Loss of +5 Volt Power to U22 Clock Ckt
G

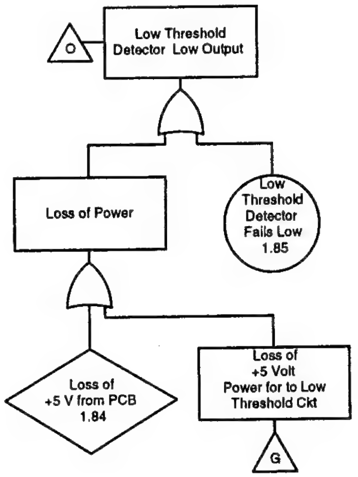
WATCHDOG TIMER COMMAND RESET FAILURE


M
Watchdog Timer Command Reset Failure
Unable to Reset WDT* with Valid SC Command
High Threshold Detector (>4 Volts) 1.126
Low Threshold Detector Low Output
PCB Interface Failure
Loss of Logic Reset Signal
Loss of Power to Low Threshold Detector Ckts
Low Threshold Detector Falls Low 1.250
PCB Broken Con- nection 1.119
PCB Interface "U18" Failure 1.120
Loss of Power to PCB Interface Circuits
Loss of +5 Volt Power for Low Threshold Ckt
G
Loss of +5 V from PCB to Low Threshold Ckt 1.118
Loss of +5 V from PCB to PCB Interface Ckts 1.121
Loss of +5 Volt Power for PCB Interface Ckt
G
WDT "U28" Failure 1.122
WDT "U20" Failure 1.123
WDT "U1" Failure 1.124
Loss of Power to Logic Reset Ckts
Loss of +5 V from PCB to Logic Ckts 1.125
Loss of +5 Volt Power for Logic Reset Ckt
G

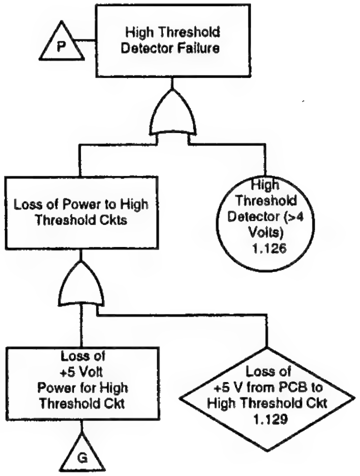
WATCHDOG TIMER AUTOMATIC RESET FAILURE


N
Automatic Reset Failure
Low Threshold Detector Low Output
WDT "U27" Failure 1.128
High Threshold Detector Failure
P
Loss of Power to Low Threshold Detector Ckts
Low Threshold Detector Fails Low 1.250
Loss of +5 V from PCB to Low Threshold Ckt 1.127
Loss of +5 Volt Power for Low Threshold Ckt
G

LOW THRESHOLD DETECTOR FAILURE

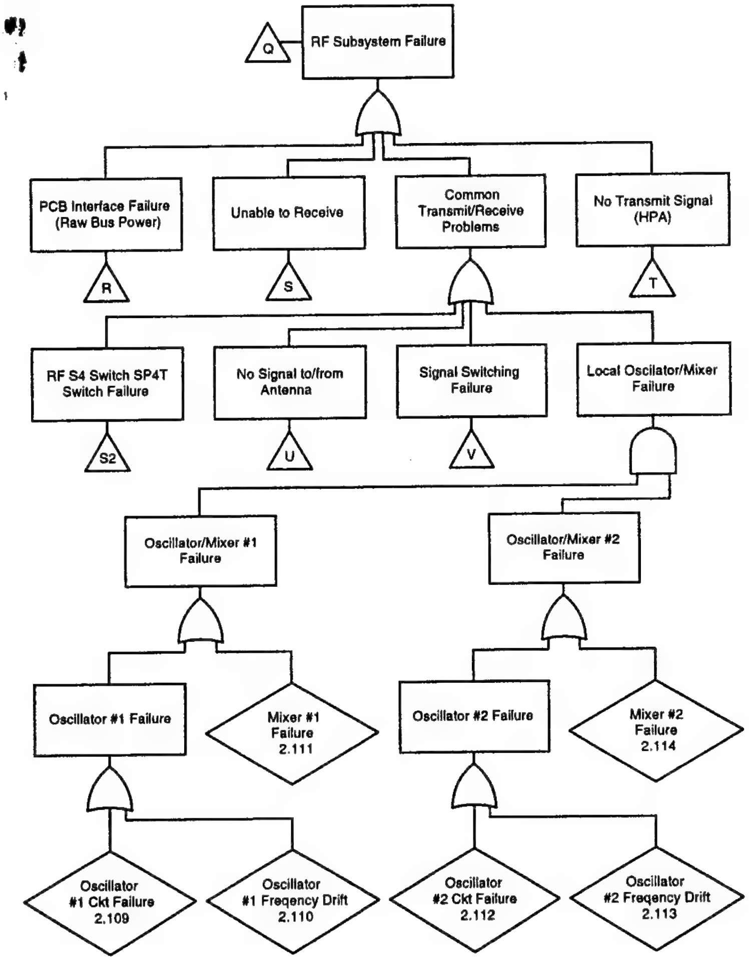

O
Low Threshold Detector Low Output
Loss of Power
Low Threshold Detector Fails Low 1.85
Loss of +5 V from PCB 1.84
Loss of +5 Volt Power for to Low Threshold Ckt
G

HIGH TRESHOLD DETECTOR FAILURE

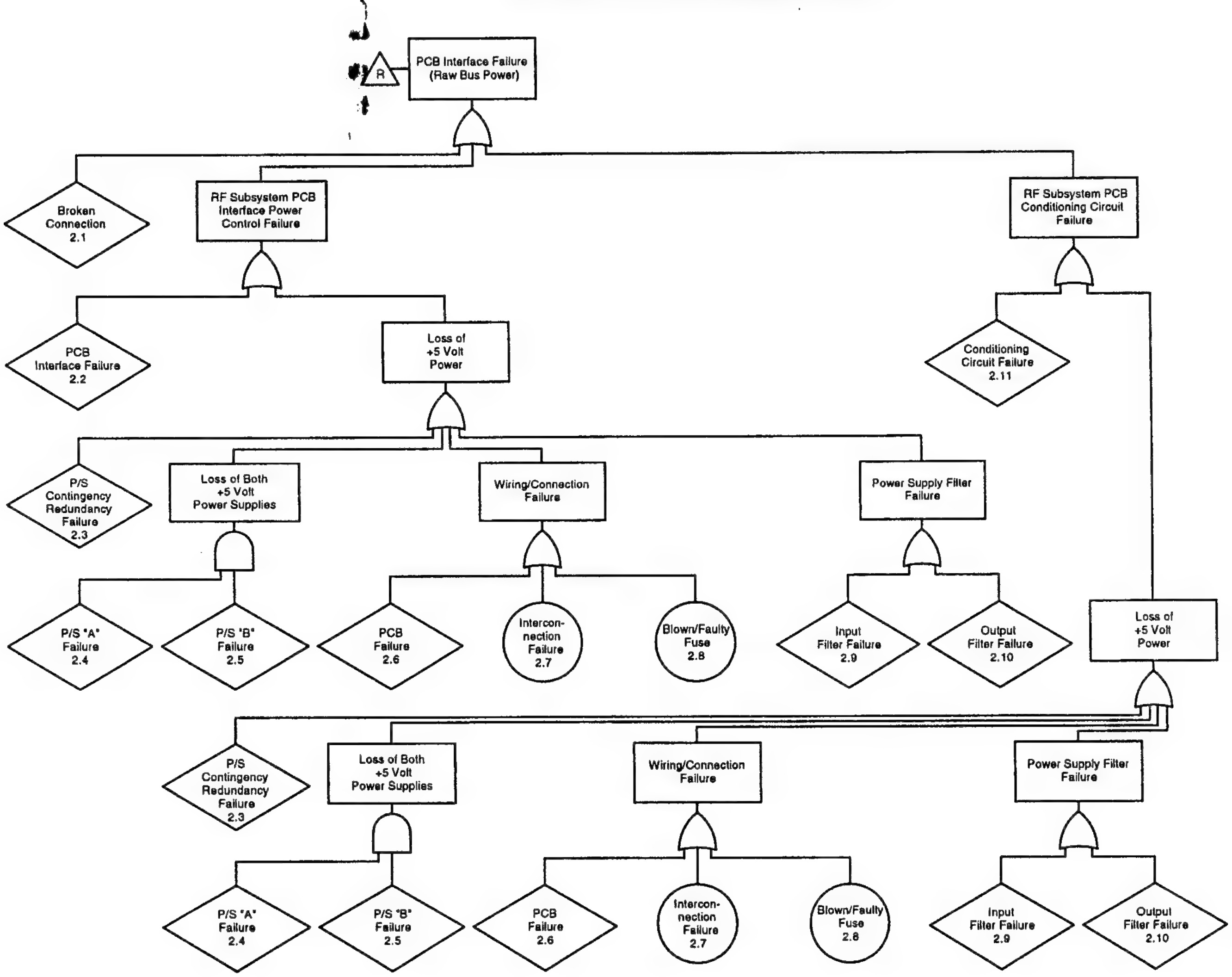

High Threshold Detector Failure
P
Loss of Power to High Threshold Ckts
High Threshold Detector (>4 Volts) 1.126
Loss of +5 Volt Power for High Threshold Ckt
G
Loss of +5 V from PCB to High Threshold Ckt 1.129

RF SUBSYSTEM FAILURE

Note: This is the top level fault tree for the RF subsystem portion

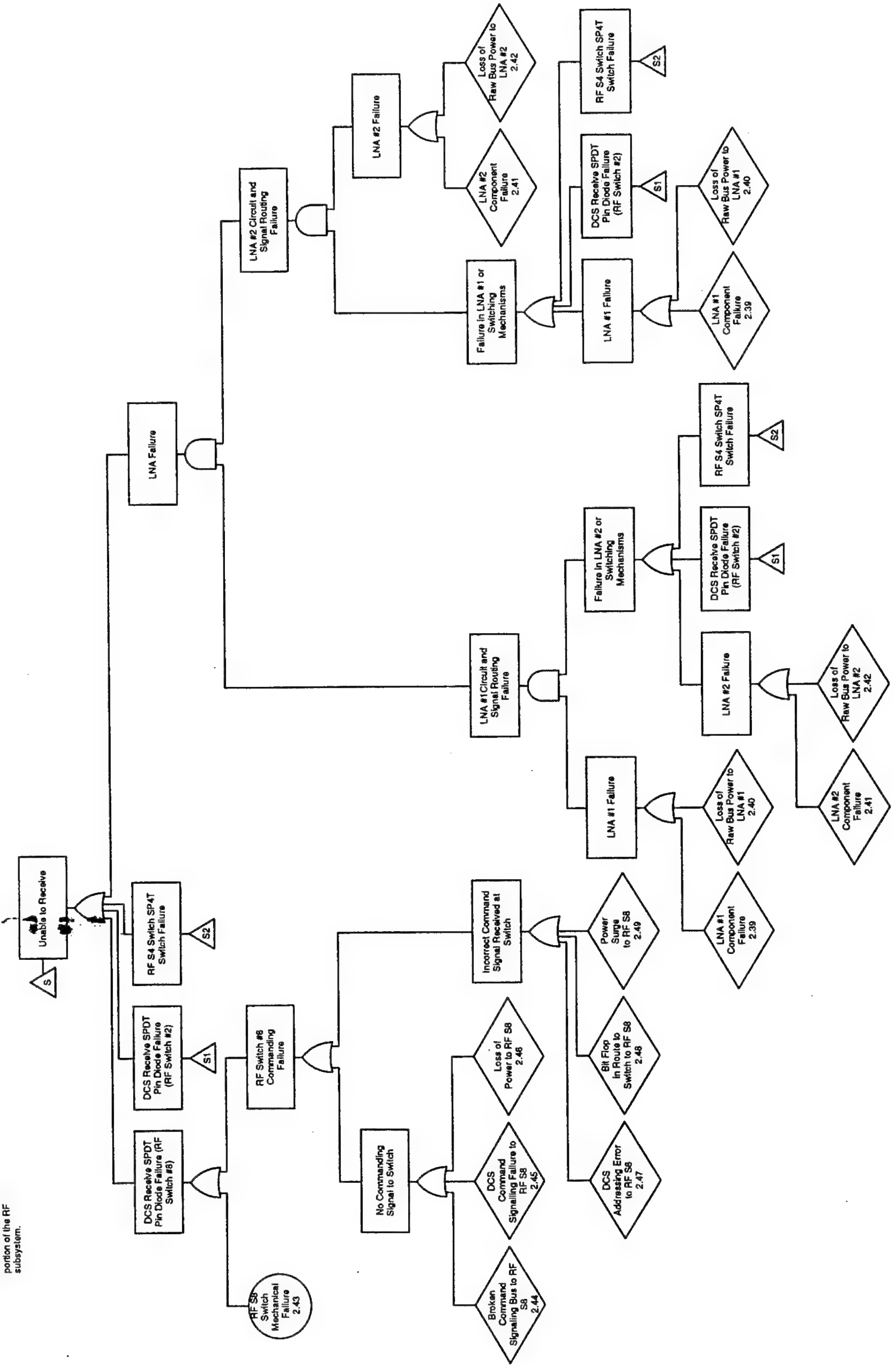

RF Subsystem Failure
Q
PCB Interface Failure (Raw Bus Power)
R
Unable to Receive
S
Common Transmit/Receive Problems
No Transmit Signal (HPA)
T
RF S4 Switch SP4T Switch Failure
S2
No Signal to/from Antenna
U
Signal Switching Failure
V
Local Oscilator/Mixer Failure
Oscillator/Mixer #1 Failure
Oscillator/Mixer #2 Failure
Oscillator #1 Failure
Mixer #1 Failure 2.111
Oscillator #2 Failure
Mixer #2 Failure 2.114
Oscillator #1 Ckt Failure 2.109
Oscillator #1 Freqency Drift 2.110
Oscillator #2 Ckt Failure 2.112
Oscillator #2 Freqency Drift 2.113

RF PCB INTERFACE CIRCUIT FAILURE

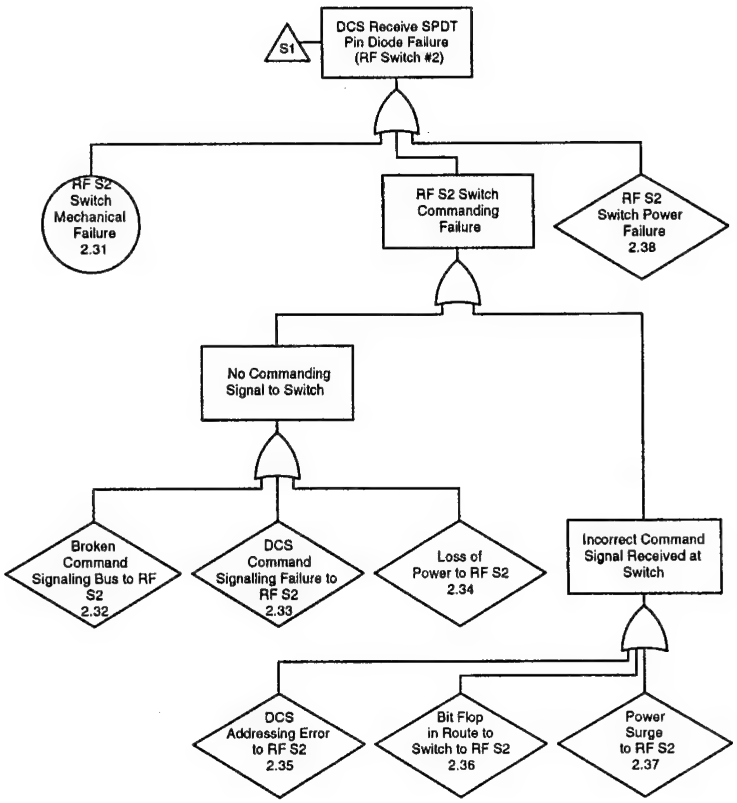

R
PCB Interface Failure (Raw Bus Power)
Broken Connection 2.1
RF Subsystem PCB Interface Power Control Failure
RF Subsystem PCB Conditioning Circuit Failure
PCB Interface Failure 2.2
Loss of +5 Volt Power
Conditioning Circuit Failure 2.11
P/S Contingency Redundancy Failure 2.3
Loss of Both +5 Volt Power Supplies
Wiring/Connection Failure
Power Supply Filter Failure
P/S "A" Failure 2.4
P/S "B" Failure 2.5
PCB Failure 2.6
Intercon-nection Failure 2.7
Blown/Faulty Fuse 2.8
Input Filter Failure 2.9
Output Filter Failure 2.10
Loss of +5 Volt Power
P/S Contingency Redundancy Failure 2.3
Loss of Both +5 Volt Power Supplies
Wiring/Connection Failure
Power Supply Filter Failure
P/S "A" Failure 2.4
P/S "B" Failure 2.5
PCB Failure 2.6
Intercon-nection Failure 2.7
Blown/Faulty Fuse 2.8
Input Filter Failure 2.9
Output Filter Failure 2.10

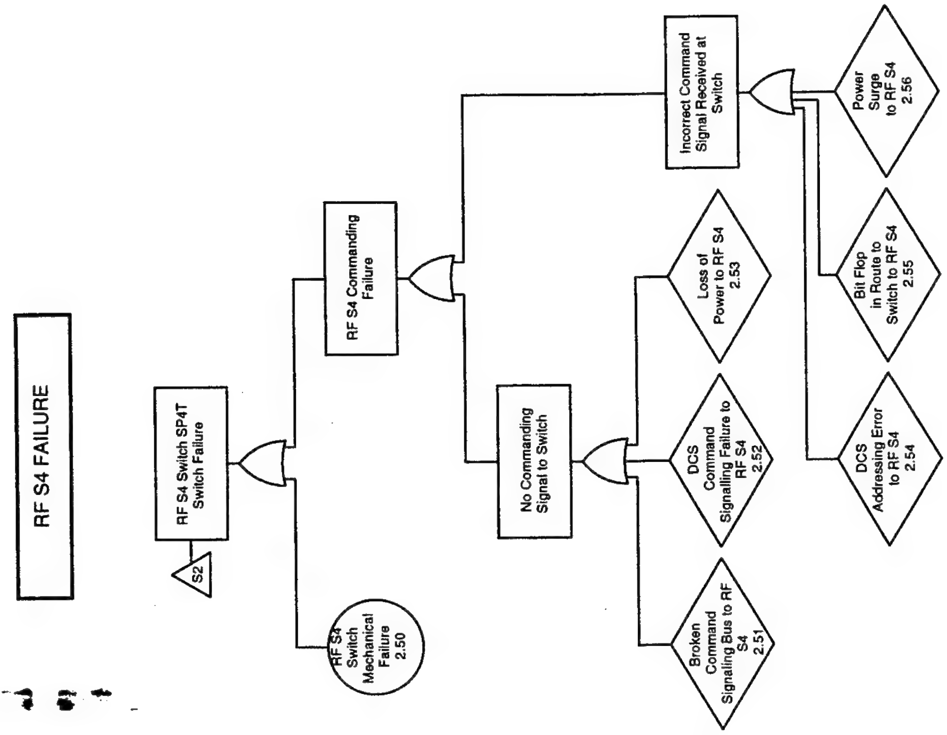
RF RECEIVER CIRCUIT FAILURE

This portion of the fault tree concerns the receiver portion of the RF subsystem.

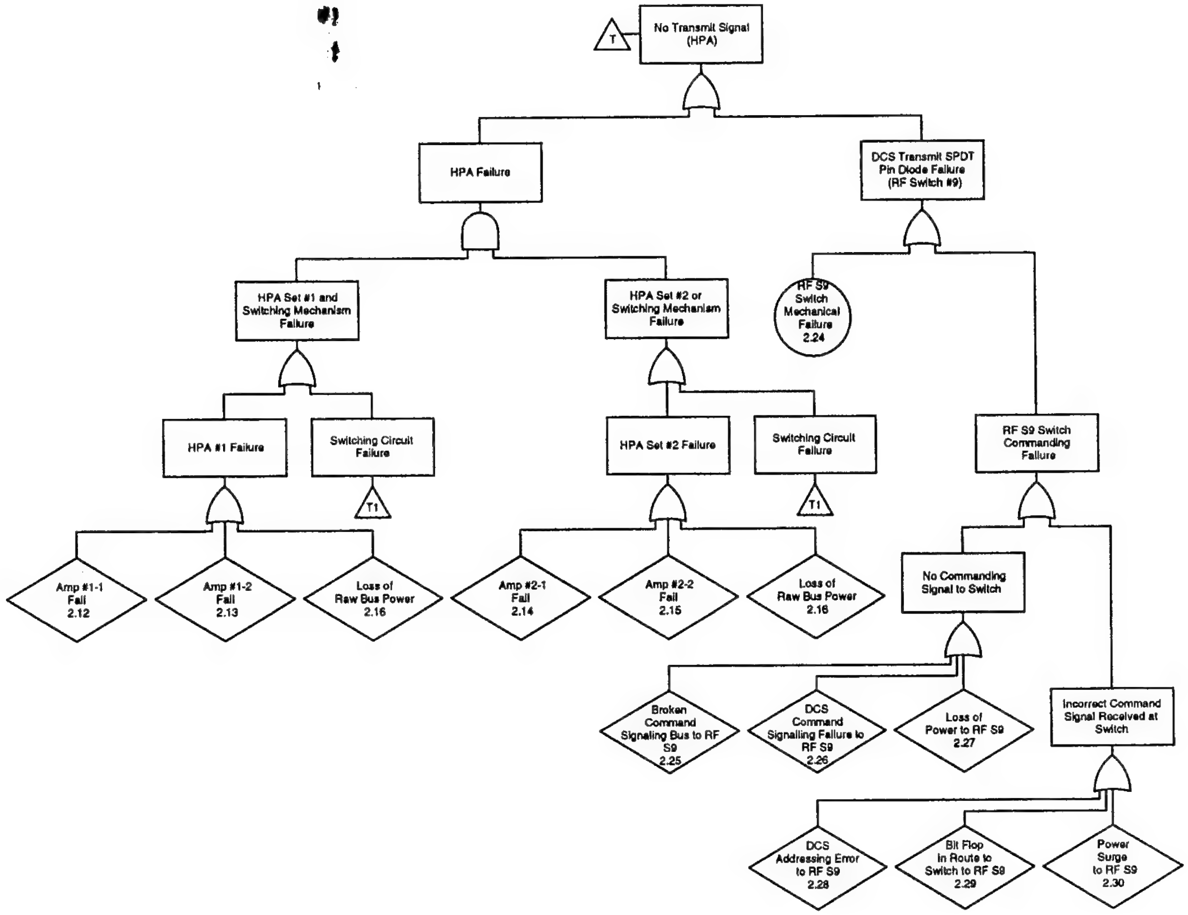

Unable to Receive
S
RF S4 Switch SP4T Switch Failure
S2
DCS Receive SPDT Pin Diode Failure (RF Switch #2)
S1
DCS Receive SPDT Pin Diode Failure (RF Switch #8)
RF S8 Switch Mechanical Failure 2.43
RF Switch #8 Commanding Failure
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S8 2.44
DCS Command Signaling Failure to RF S8 2.45
Loss of Power to RF S8 2.46
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S8 2.47
Bit Flop In Route to Switch to RF S8 2.48
Power Surge to RF S8 2.49
LNA Failure
LNA #1 Circuit and Signal Routing Failure
LNA #1 Failure
LNA #1 Component Failure 2.39
Loss of Raw Bus Power to LNA #1 2.40
Failure in LNA #2 or Switching Mechanisms
LNA #2 Failure
LNA #2 Component Failure 2.41
Loss of Raw Bus Power to LNA #2 2.42
DCS Receive SPDT Pin Diode Failure (RF Switch #2)
S1
RF S4 Switch SP4T Switch Failure
S2
LNA #2 Circuit and Signal Routing Failure
Failure in LNA #1 or Switching Mechanisms
LNA #1 Failure
LNA #1 Component Failure 2.39
Loss of Raw Bus Power to LNA #1 2.40
DCS Receive SPDT Pin Diode Failure (RF Switch #2)
S1
RF S4 Switch SP4T Switch Failure
S2
LNA #2 Failure
LNA #2 Component Failure 2.41
Loss of Raw Bus Power to LNA #2 2.42

RF S2 FAILURE


S1
DCS Receive SPDT Pin Diode Failure (RF Switch #2)
RF S2 Switch Mechanical Failure 2.31
RF S2 Switch Commanding Failure
RF S2 Switch Power Failure 2.38
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S2 2.32
DCS Command Signalling Failure to RF S2 2.33
Loss of Power to RF S2 2.34
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S2 2.35
Bit Flop in Route to Switch to RF S2 2.36
Power Surge to RF S2 2.37

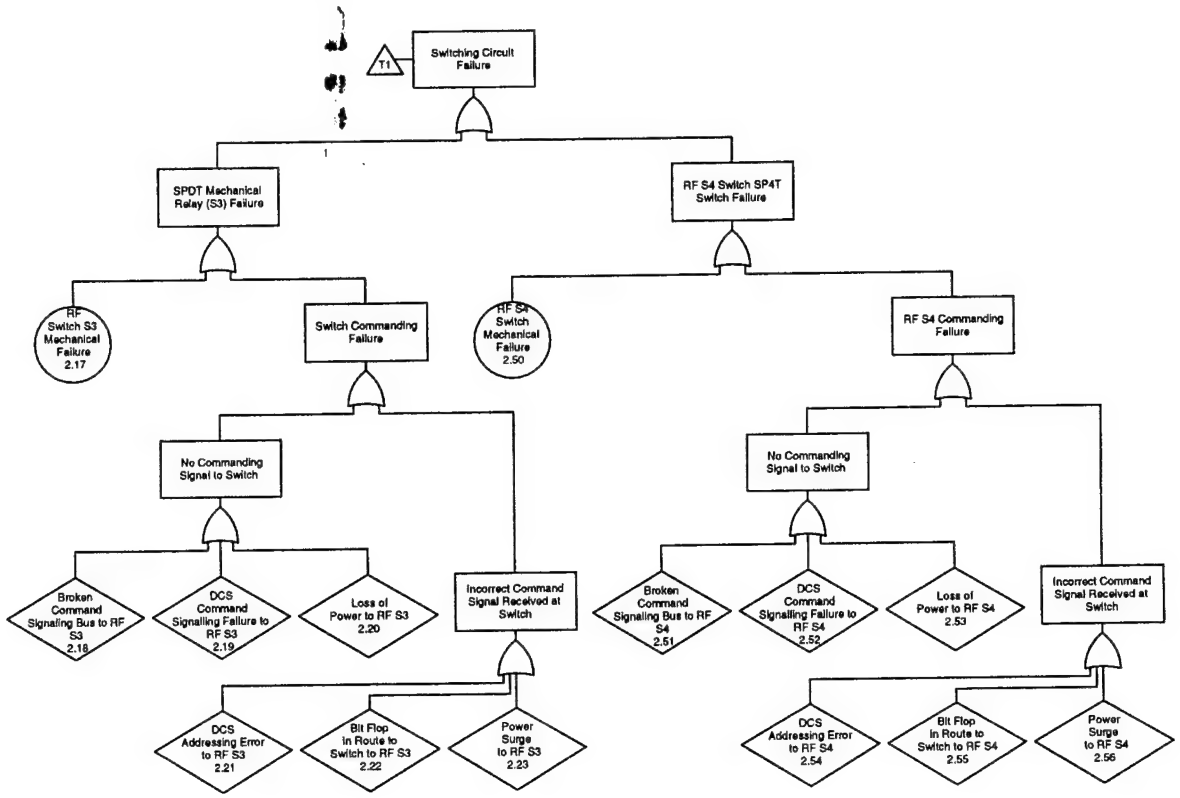

RF S4 FAILURE
RF S4 Switch SP4T Switch Failure
S2
RF S4 Switch Mechanical Failure 2.50
RF S4 Commanding Failure
No Commanding Signal to Switch
Incorrect Command Signal Received at Switch
Broken Command Signaling Bus to RF S4 2.51
DCS Command Signalling Failure to RF S4 2.52
Loss of Power to RF S4 2.53
DCS Addressing Error to RF S4 2.54
Bit Flop in Route to Switch to RF S4 2.55
Power Surge to RF S4 2.56

RF TRANSMITTER CIRCUIT FAILURE

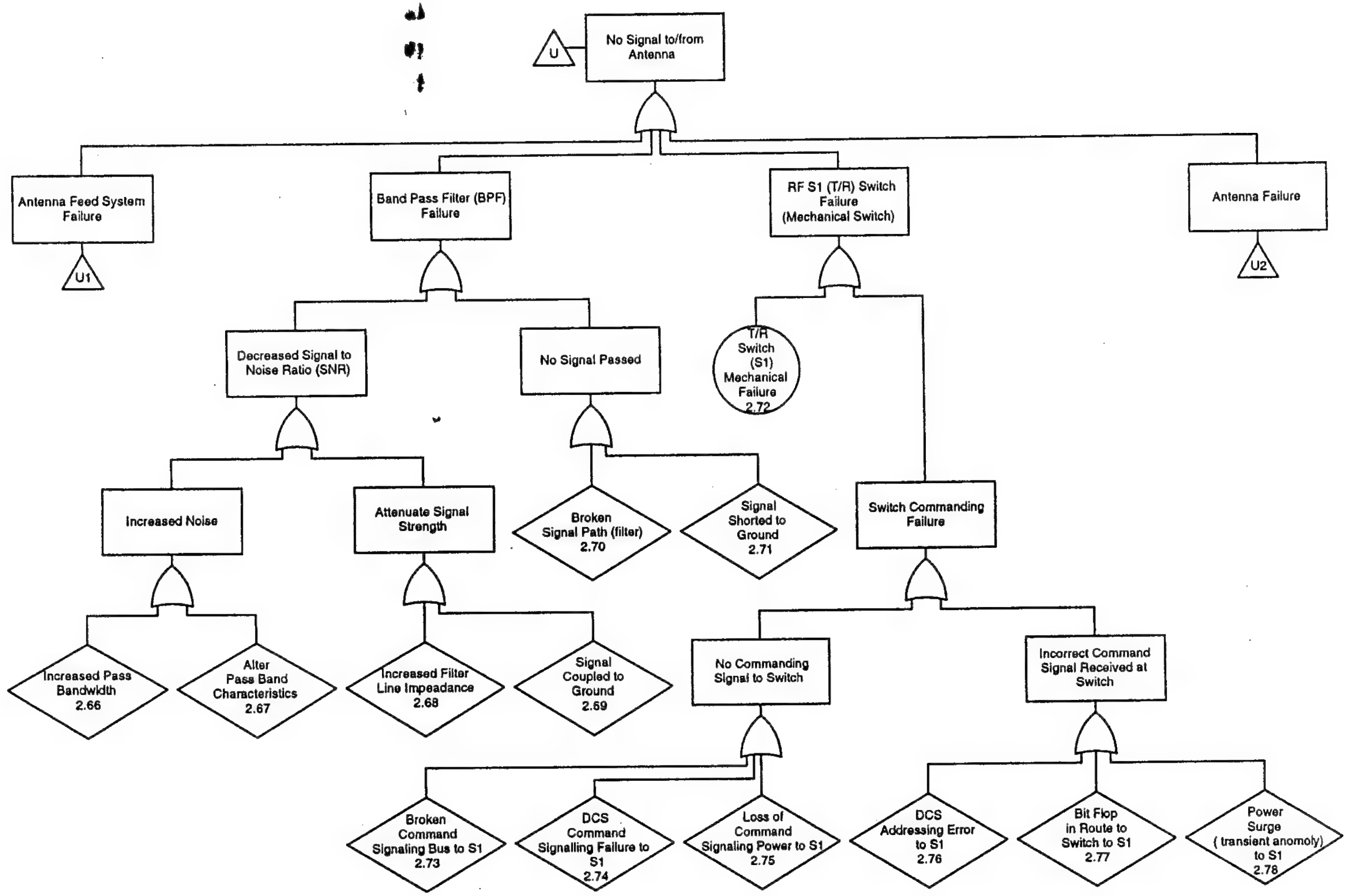


T
No Transmit Signal (HPA)
HPA Failure
DCS Transmit SPDT Pin Diode Failure (RF Switch #9)
HPA Set #1 and Switching Mechanism Failure
HPA Set #2 or Switching Mechanism Failure
RF S9 Switch Mechanical Failure 2.24
HPA #1 Failure
Switching Circuit Failure
T1
HPA Set #2 Failure
Switching Circuit Failure
T1
RF S9 Switch Commanding Failure
Amp #1-1 Fail 2.12
Amp #1-2 Fail 2.13
Loss of Raw Bus Power 2.16
Amp #2-1 Fail 2.14
Amp #2-2 Fail 2.15
Loss of Raw Bus Power 2.16
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S9 2.25
DCS Command Signalling Failure to RF S9 2.26
Loss of Power to RF S9 2.27
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S9 2.28
Bit Flop In Route to Switch to RF S9 2.29
Power Surge to RF S9 2.30

RF TRANSMITTER CIRCUIT SWITCHING FAILURE

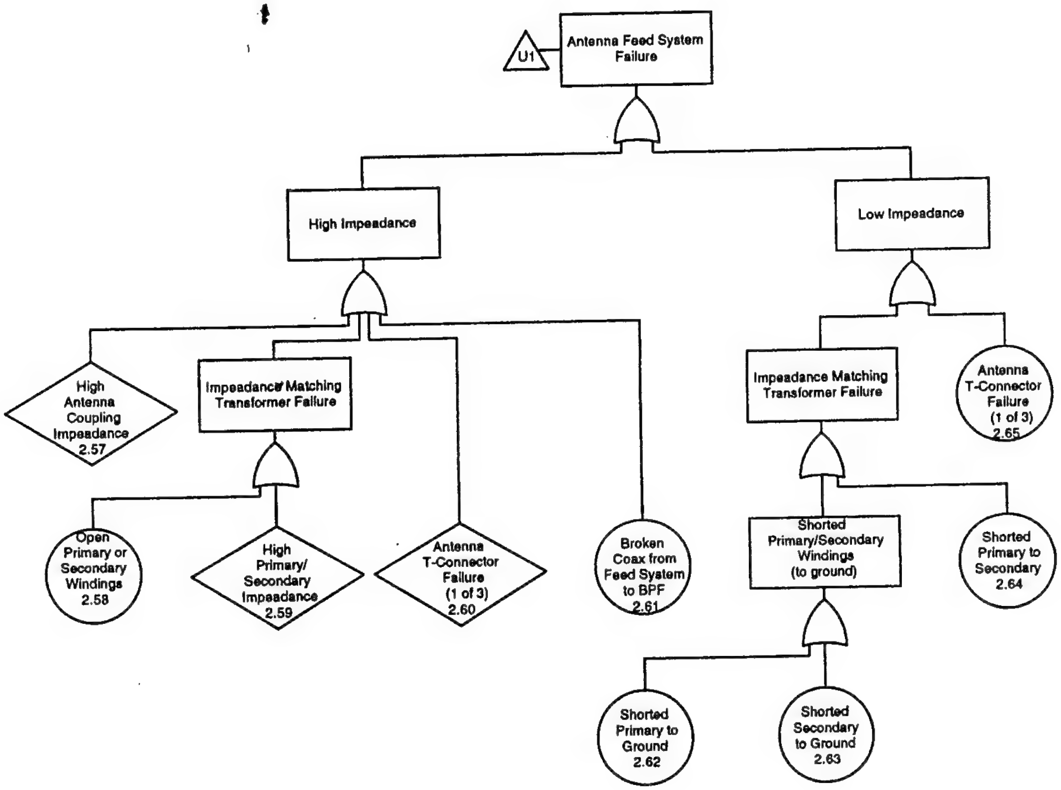

Switching Circuit Failure
T1
SPDT Mechanical Relay (S3) Failure
RF S4 Switch SP4T Switch Failure
RF Switch S3 Mechanical Failure 2.17
Switch Commanding Failure
RF S4 Switch Mechanical Failure 2.50
RF S4 Commanding Failure
No Commanding Signal to Switch
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S3 2.18
DCS Command Signalling Failure to RF S3 2.19
Loss of Power to RF S3 2.20
Incorrect Command Signal Received at Switch
Broken Command Signaling Bus to RF S4 2.51
DCS Command Signalling Failure to RF S4 2.52
Loss of Power to RF S4 2.53
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S3 2.21
Bit Flop in Route to Switch to RF S3 2.22
Power Surge to RF S3 2.23
DCS Addressing Error to RF S4 2.54
Bit Flop in Route to Switch to RF S4 2.55
Power Surge to RF S4 2.56

ANTENNA CIRCUIT FAILURE



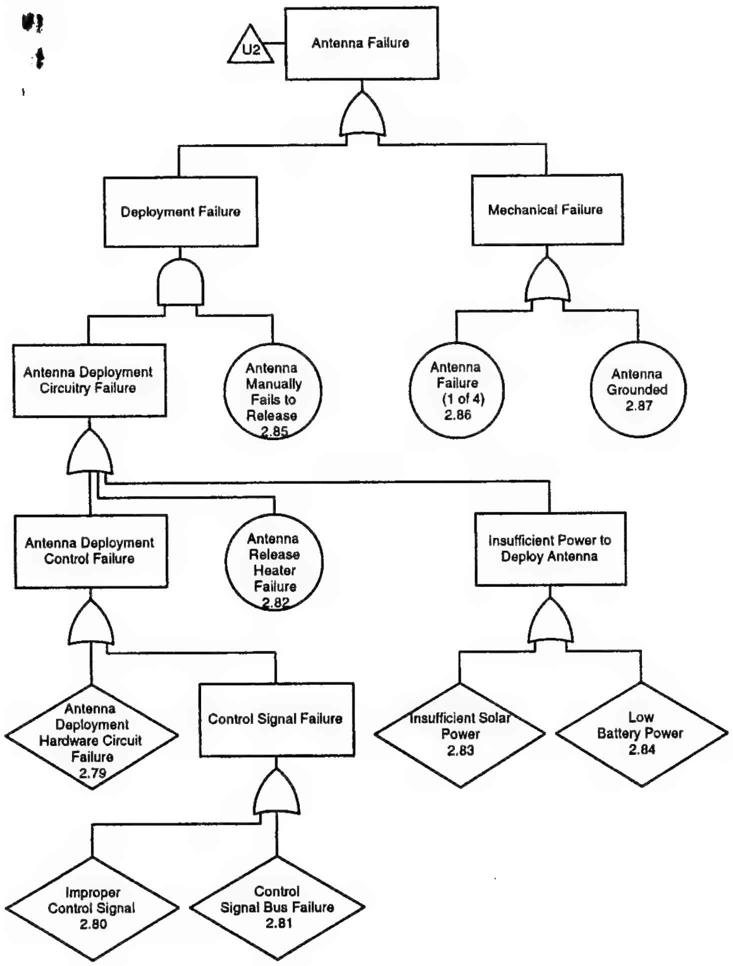
U
No Signal to/from Antenna
Antenna Feed System Failure
U1
Band Pass Filter (BPF) Failure
RF S1 (T/R) Switch Failure (Mechanical Switch)
Antenna Failure
U2
Decreased Signal to Noise Ratio (SNR)
No Signal Passed
T/R Switch (S1) Mechanical Failure 2.72
Increased Noise
Attenuate Signal Strength
Broken Signal Path (filter) 2.70
Signal Shorted to Ground 2.71
Switch Commanding Failure
Increased Pass Bandwidth 2.66
Alter Pass Band Characteristics 2.67
Increased Filter Line Impeadance 2.68
Signal Coupled to Ground 2.69
No Commanding Signal to Switch
Incorrect Command Signal Received at Switch
Broken Command Signaling Bus to S1 2.73
DCS Command Signalling Failure to S1 2.74
Loss of Command Signaling Power to S1 2.75
DCS Addressing Error to S1 2.76
Bit Flop in Route to Switch to S1 2.77
Power Surge (transient anomoly) to S1 2.78

ANTENNA FEED SYSTEM FAILURE

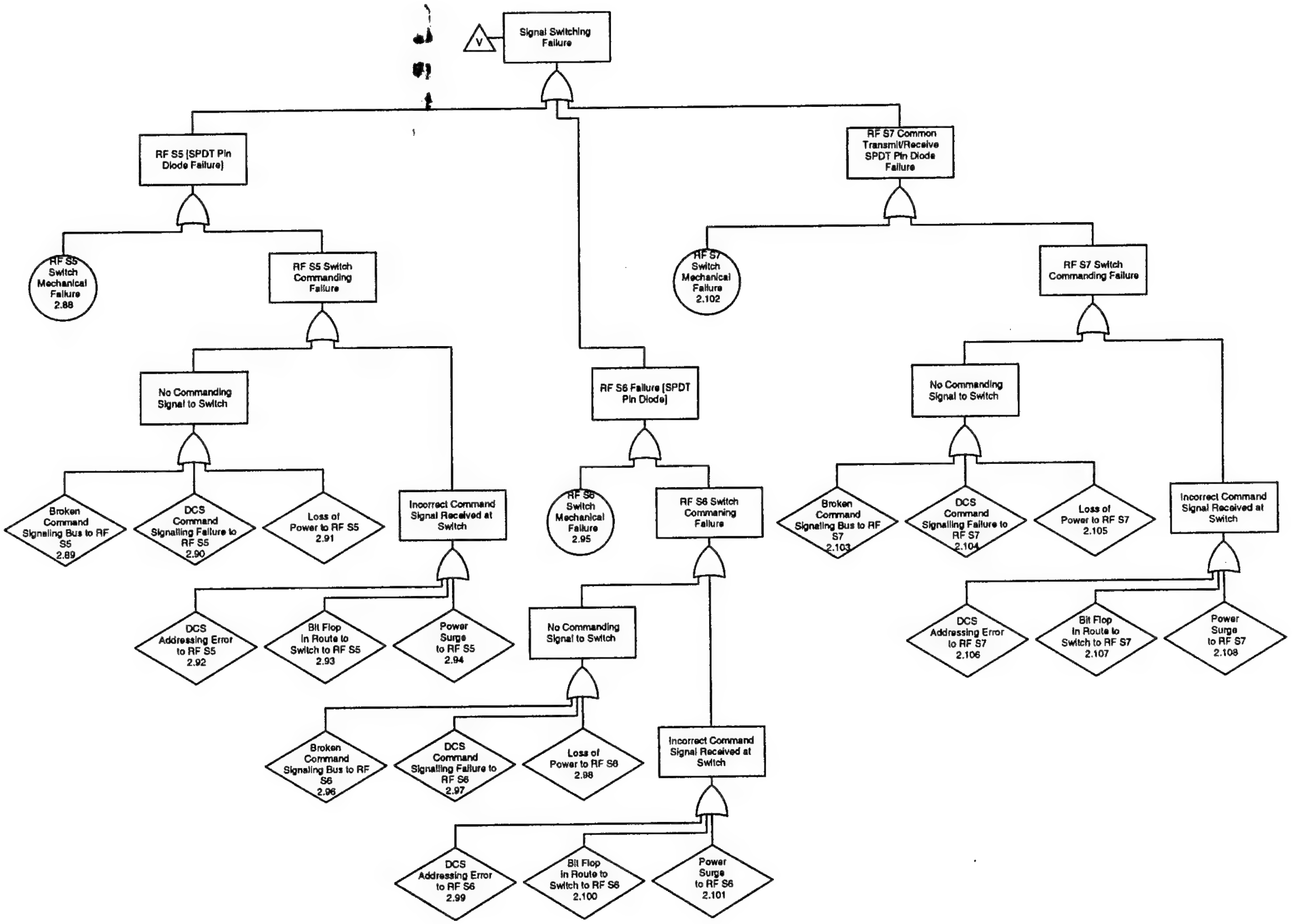

U1
Antenna Feed System Failure
High Impeadance
Low Impeadance
High Antenna Coupling Impeadance 2.57
Impeadance Matching Transformer Failure
Antenna T-Connector Failure (1 of 3) 2.60
Broken Coax from Feed System to BPF 2.61
Open Primary or Secondary Windings 2.58
High Primary/ Secondary Impeadance 2.59
Impeadance Matching Transformer Failure
Antenna T-Connector Failure (1 of 3) 2.65
Shorted Primary/Secondary Windings (to ground)
Shorted Primary to Secondary 2.64
Shorted Primary to Ground 2.62
Shorted Secondary to Ground 2.63

ANTENNA FAILURE

Note: This portion of the fault tree deals with the failure of the antenna or antenna deployment. Failure event 2.84 may not be a viable event since battery power is not the normal source for antenna deployment.

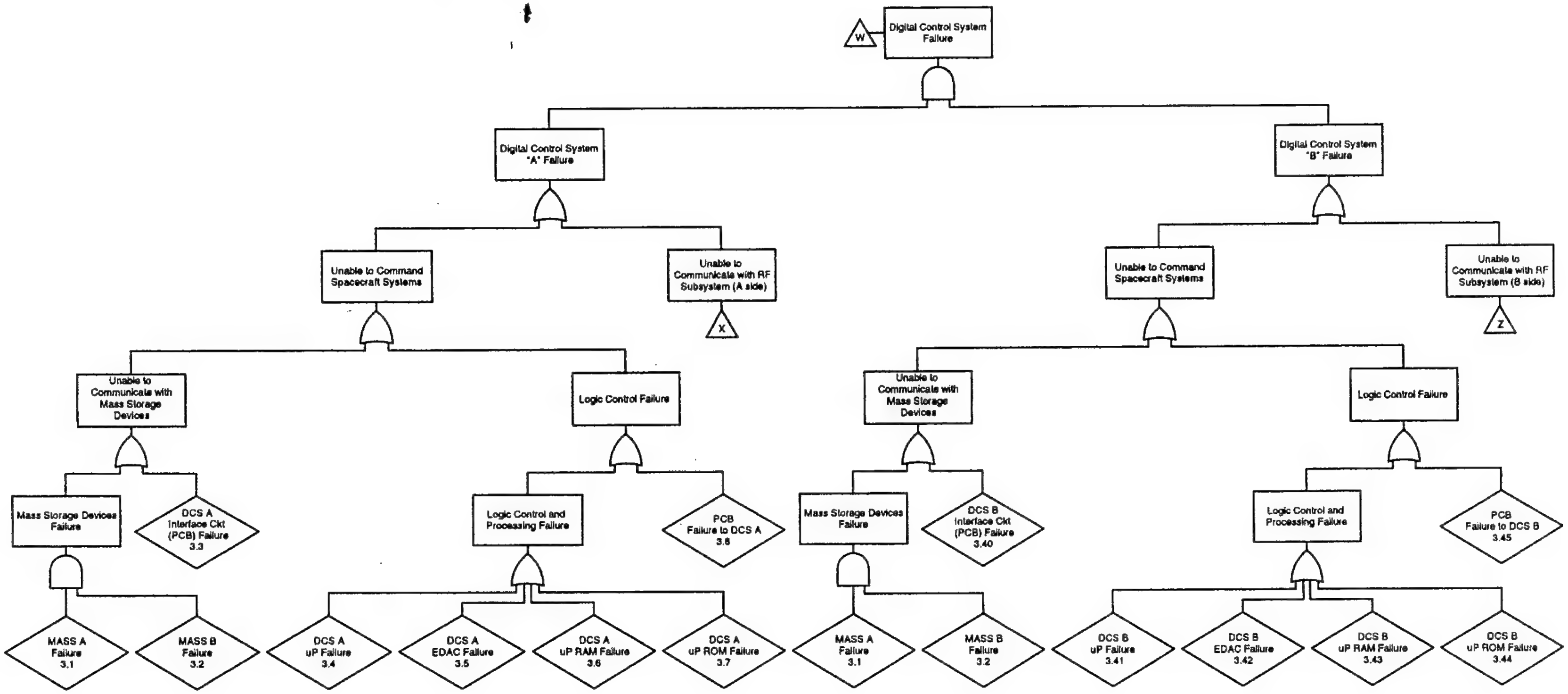

U2
Antenna Failure
Deployment Failure
Mechanical Failure
Antenna Deployment Circuitry Failure
Antenna Manually Fails to Release 2.85
Antenna Failure (1 of 4) 2.86
Antenna Grounded 2.87
Antenna Deployment Control Failure
Antenna Release Heater Failure 2.82
Insufficient Power to Deploy Antenna
Antenna Deployment Hardware Circuit Failure 2.79
Control Signal Failure
Insufficient Solar Power 2.83
Low Battery Power 2.84
Improper Control Signal 2.80
Control Signal Bus Failure 2.81

RF SIGNAL SWITCHING FAILURE


V
Signal Switching Failure
RF S5 [SPDT Pin Diode Failure]
RF S5 Switch Mechanical Failure 2.88
RF S5 Switch Commanding Failure
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S5 2.89
DCS Command Signalling Failure to RF S5 2.90
Loss of Power to RF S5 2.91
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S5 2.92
Bit Flop In Route to Switch to RF S5 2.93
Power Surge to RF S5 2.94
RF S6 Failure [SPDT Pin Diode]
RF S6 Switch Mechanical Failure 2.95
RF S6 Switch Commaning Failure
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S6 2.96
DCS Command Signalling Failure to RF S6 2.97
Loss of Power to RF S6 2.98
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S6 2.99
Bit Flop In Route to Switch to RF S6 2.100
Power Surge to RF S6 2.101
RF S7 Common Transmit/Receive SPDT Pin Diode Failure
RF S7 Switch Mechanical Failure 2.102
RF S7 Switch Commanding Failure
No Commanding Signal to Switch
Broken Command Signaling Bus to RF S7 2.103
DCS Command Signalling Failure to RF S7 2.104
Loss of Power to RF S7 2.105
Incorrect Command Signal Received at Switch
DCS Addressing Error to RF S7 2.106
Bit Flop In Route to Switch to RF S7 2.107
Power Surge to RF S7 2.108

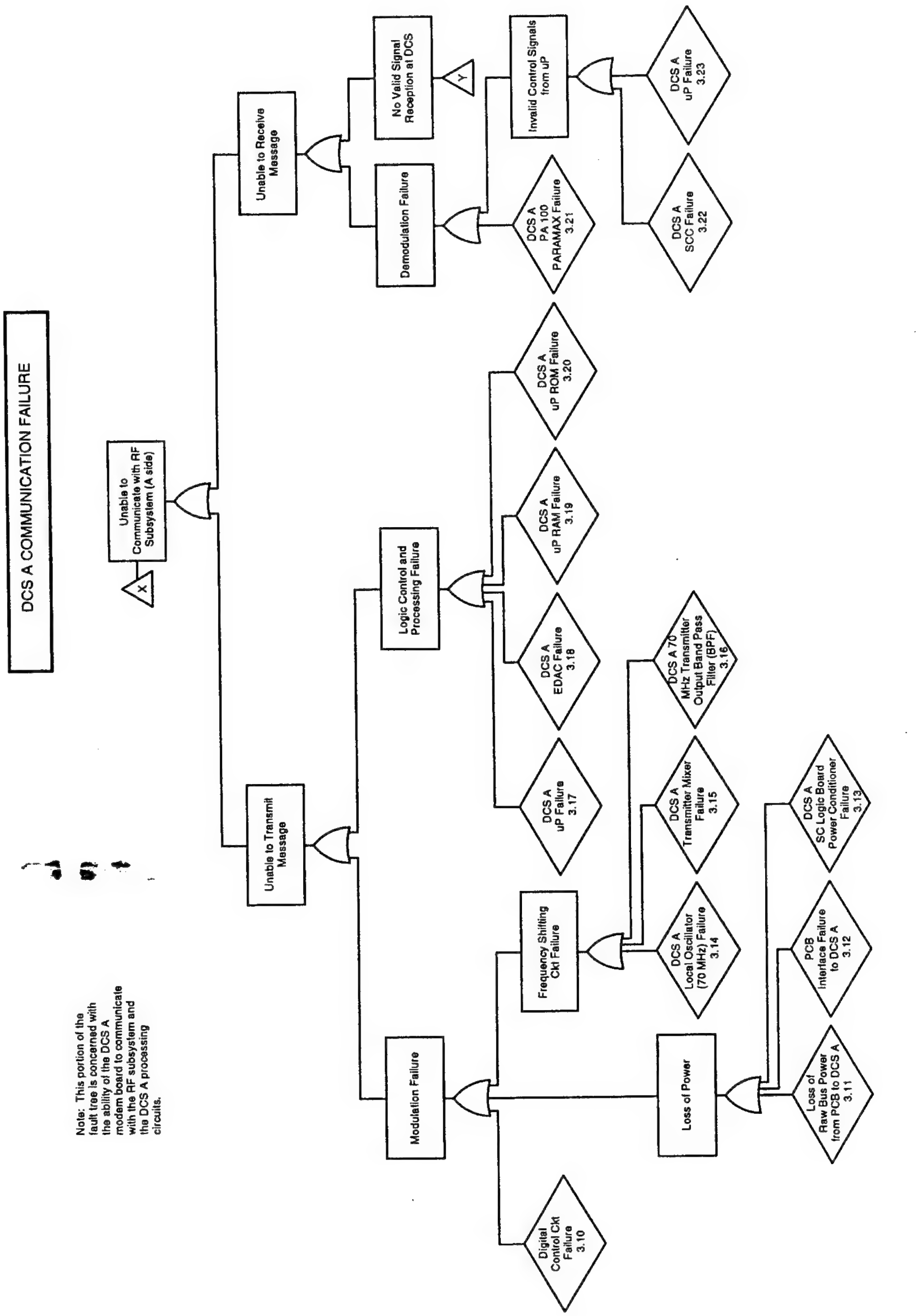
Digital Control Subsystem Failure

Note: This is the top level of the DCS portion of the fault tree.



W
Digital Control System Failure
Digital Control System "A" Failure
Digital Control System "B" Failure
Unable to Command Spacecraft Systems
Unable to Communicate with RF Subsystem (A side)
X
Unable to Command Spacecraft Systems
Unable to Communicate with RF Subsystem (B side)
Z
Unable to Communicate with Mass Storage Devices
Logic Control Failure
Unable to Communicate with Mass Storage Devices
Logic Control Failure
Mass Storage Devices Failure
DCS A Interface Ckt (PCB) Failure 3.3
Logic Control and Processing Failure
PCB Failure to DCS A 3.8
Mass Storage Devices Failure
DCS B Interface Ckt (PCB) Failure 3.40
Logic Control and Processing Failure
PCB Failure to DCS B 3.45
MASS A Failure 3.1
MASS B Failure 3.2
DCS A uP Failure 3.4
DCS A EDAC Failure 3.5
DCS A uP RAM Failure 3.6
DCS A uP ROM Failure 3.7
MASS A Failure 3.1
MASS B Failure 3.2
DCS B uP Failure 3.41
DCS B EDAC Failure 3.42
DCS B uP RAM Failure 3.43
DCS B uP ROM Failure 3.44

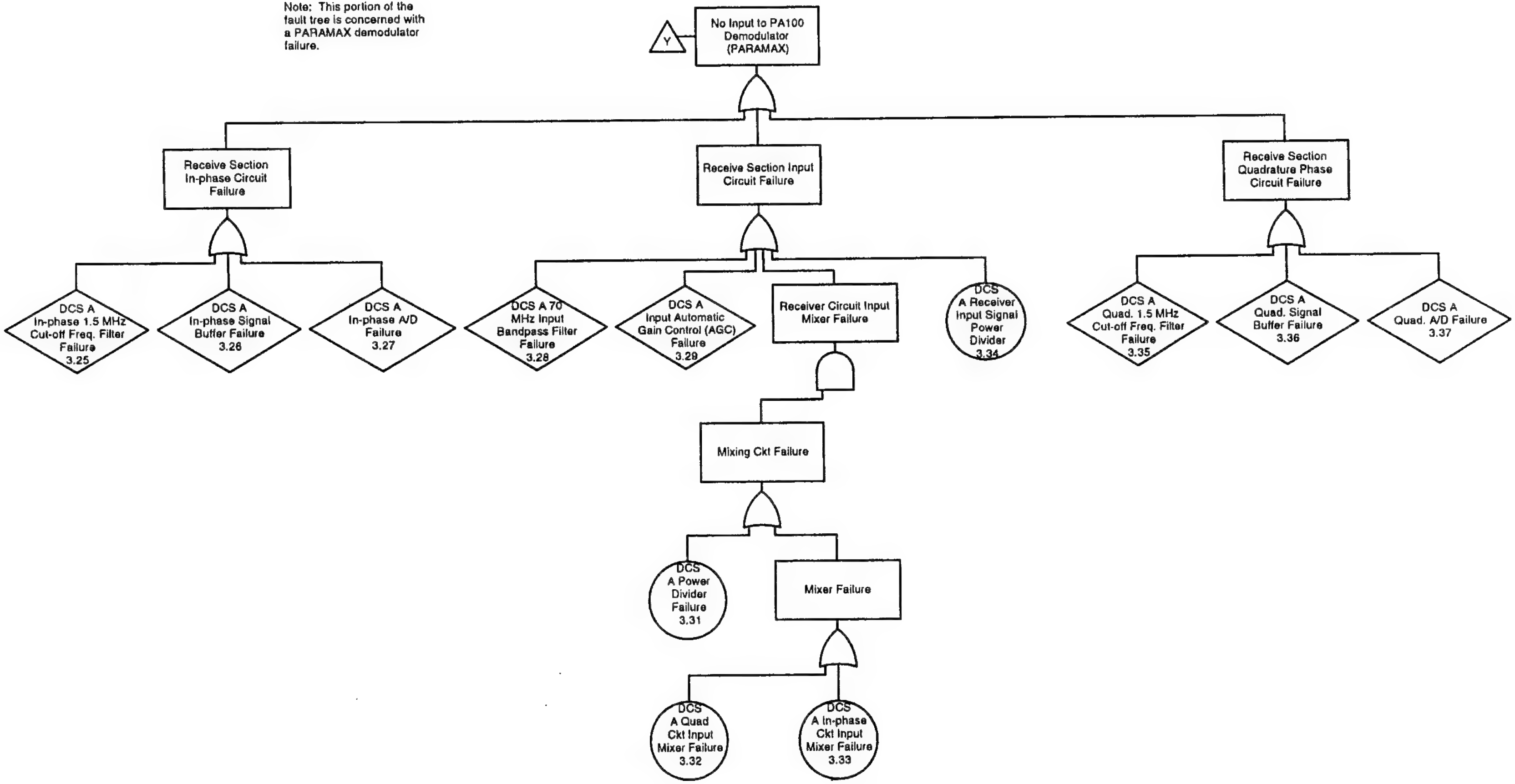
DCS A COMMUNICATION FAILURE


Unable to Communicate with RF Subsystem (A side)
X
Unable to Transmit Message
Unable to Receive Message
Modulation Failure
Logic Control and Processing Failure
Demodulation Failure
No Valid Signal Reception at DCS
Y
Invalid Control Signals from uP
Digital Control Ckt Failure 3.10
Loss of Power
Frequency Shifting Ckt Failure
Loss of Raw Bus Power from PCB to DCS A 3.11
PCB Interface Failure to DCS A 3.12
DCS A SC Logic Board Power Conditioner Failure 3.13
DCS A Local Oscillator (70 MHz) Failure 3.14
DCS A Transmitter Mixer Failure 3.15
DCS A 70 MHz Transmitter Output Band Pass Filter (BPF) 3.16
DCS A uP Failure 3.17
DCS A EDAC Failure 3.18
DCS A uP RAM Failure 3.19
DCS A uP ROM Failure 3.20
DCS A PA 100 PARAMAX Failure 3.21
DCS A SCC Failure 3.22
DCS A uP Failure 3.23

Note: This portion of the fault tree is concerned with the ability of the DCS A modem board to communicate with the RF subsystem and the DCS A processing circuits.

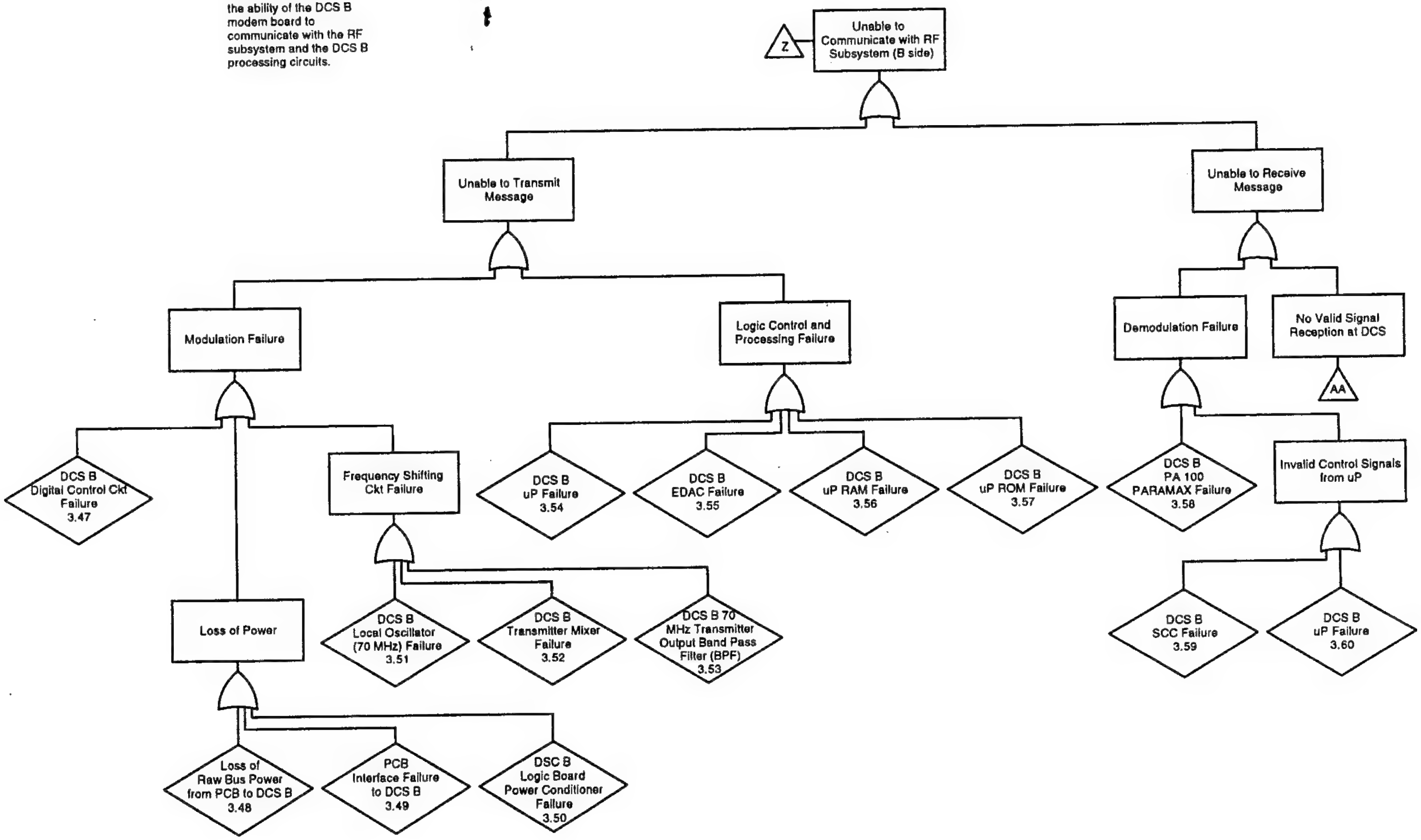
DCS A MODEM BOARD FAILURE

Note: This portion of the fault tree is concerned with a PARAMAX demodulator failure.


Y
No Input to PA100 Demodulator (PARAMAX)
Receive Section In-phase Circuit Failure
Receive Section Input Circuit Failure
Receive Section Quadrature Phase Circuit Failure
DCS A In-phase 1.5 MHz Cut-off Freq. Filter Failure 3.25
DCS A In-phase Signal Buffer Failure 3.26
DCS A In-phase A/D Failure 3.27
DCS A 70 MHz Input Bandpass Filter Failure 3.28
DCS A Input Automatic Gain Control (AGC) Failure 3.29
Receiver Circuit Input Mixer Failure
DCS A Receiver Input Signal Power Divider 3.34
DCS A Quad. 1.5 MHz Cut-off Freq. Filter Failure 3.35
DCS A Quad. Signal Buffer Failure 3.36
DCS A Quad. A/D Failure 3.37
Mixing Ckt Failure
DCS A Power Divider Failure 3.31
Mixer Failure
DCS A Quad Ckt Input Mixer Failure 3.32
DCS A In-phase Ckt Input Mixer Failure 3.33

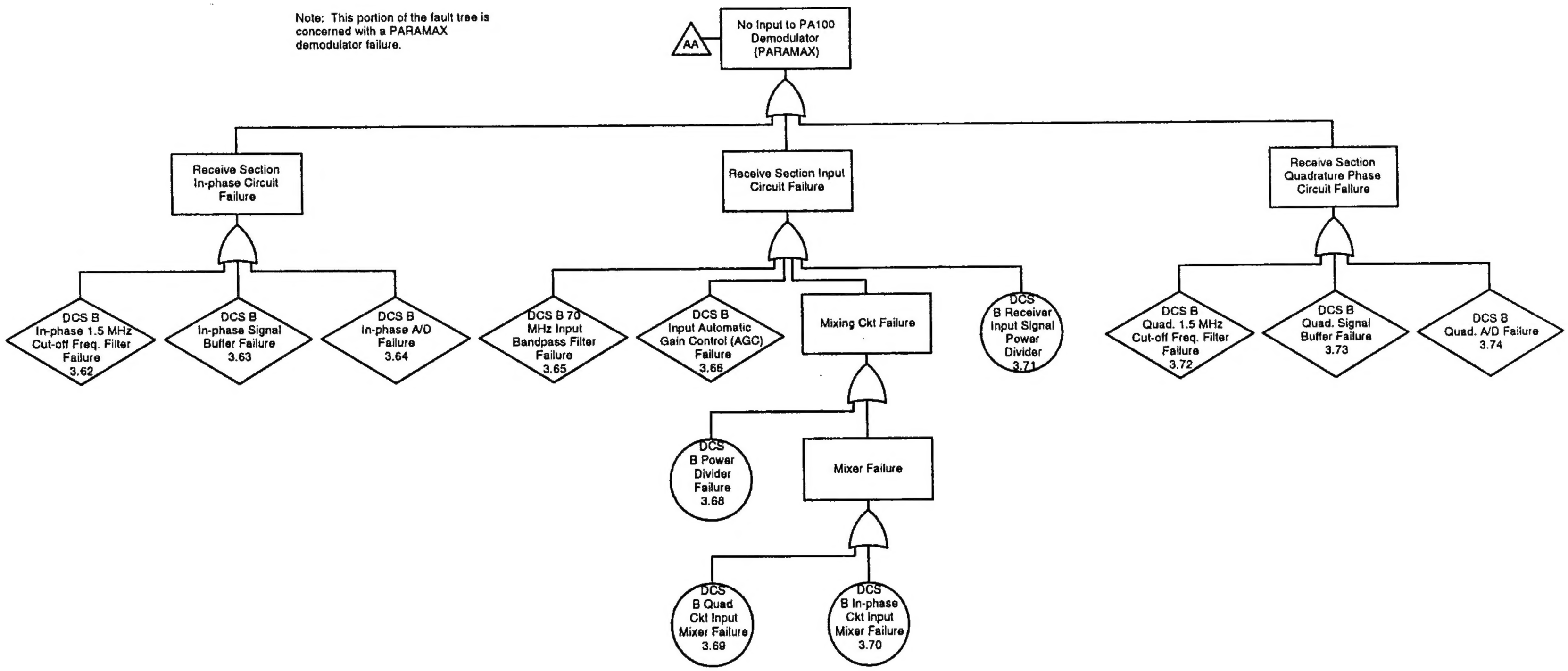
DCS B COMMUNICATION FAILURE

Note: This portion of the fault tree is concerned with the ability of the DCS B modem board to communicate with the RF subsystem and the DCS B processing circuits.


Z
Unable to Communicate with RF Subsystem (B side)
Unable to Transmit Message
Unable to Receive Message
Modulation Failure
Logic Control and Processing Failure
Demodulation Failure
No Valid Signal Reception at DCS
AA
DCS B Digital Control Ckt Failure 3.47
Frequency Shifting Ckt Failure
DCS B uP Failure 3.54
DCS B EDAC Failure 3.55
DCS B uP RAM Failure 3.56
DCS B uP ROM Failure 3.57
DCS B PA 100 PARAMAX Failure 3.58
Invalid Control Signals from uP
Loss of Power
DCS B Local Oscillator (70 MHz) Failure 3.51
DCS B Transmitter Mixer Failure 3.52
DCS B 70 MHz Transmitter Output Band Pass Filter (BPF) 3.53
DCS B SCC Failure 3.59
DCS B uP Failure 3.60
Loss of Raw Bus Power from PCB to DCS B 3.48
PCB Interface Failure to DCS B 3.49
DSC B Logic Board Power Conditioner Failure 3.50

DCS B MODEM BOARD FAILURE

Note: This portion of the fault tree is concerned with a PARAMAX demodulator failure.


AA
No Input to PA100 Demodulator (PARAMAX)
Receive Section In-phase Circuit Failure
Receive Section Input Circuit Failure
Receive Section Quadrature Phase Circuit Failure
DCS B In-phase 1.5 MHz Cut-off Freq. Filter Failure 3.62
DCS B In-phase Signal Buffer Failure 3.63
DCS B In-phase A/D Failure 3.64
DCS B 70 MHz Input Bandpass Filter Failure 3.65
DCS B Input Automatic Gain Control (AGC) Failure 3.66
Mixing Ckt Failure
DCS B Receiver Input Signal Power Divider 3.71
DCS B Quad. 1.5 MHz Cut-off Freq. Filter Failure 3.72
DCS B Quad. Signal Buffer Failure 3.73
DCS B Quad. A/D Failure 3.74
DCS B Power Divider Failure 3.68
Mixer Failure
DCS B Quad Ckt Input Mixer Failure 3.69
DCS B In-phase Ckt Input Mixer Failure 3.70

LIST OF REFERENCES

1. Hand, G. F., *Intermediate Design and Analysis of the PANSAT Electrical Power Subsystem,* Master's Thesis Naval Postgraduate School, March 1994

2. Birolini, A., "Design for Reliability", Chapter 29 of book edited by Kusiak, A., *Concurrent Engineering: Automation, Tools, and Techniques*, John Wiley and Sons, Inc., 1993

3. Horning, J. A., "Navy Education Through Amateur Satellite Development", Naval Postgraduate School, 1993

4. Barlow, R. E., Lambert, H. E., "Introduction to Fault Tree Analysis", from *Reliability and Fault Tree Analysis*, edited by Barlow, R. E., Fussell, J. B., and Singpurwalla, N. D., Society for Industrial and Applied Mathematics, 1975

5. Roland, H. E., Moriarty, B., *System Safety Engineering and Management*, John Wiley and Sons, Inc., 1990

6. Esary, J. D., *An Introduction to Coherent Systems and Positive Component Dependence*, 1995

7. Youngren, M., Course notes: OA 4302 Reliability and Weapon System Effectiveness Measurement, Naval Postgraduate School, 1995

8. Keeble, T. G., *Fault Tree Reliability Analysis of the Naval Postgraduate School Mini-satellite (ORION)*, Master's Thesis Naval Postgraduate School, September 1987

9. FaultREASE Version 1.2 User's Manual, Arthur D. Little, Inc., 1993

10. Sakoda, D., "Effective Area of a Tumbling PANSAT for Solar Flux", SSAG-D-PA003, Naval Postgraduate School, August 1994

11. Department of Defense Military Standard MIL-STD-785B, *Reliability Program for Systems and Equipment Development and Production*, 1980

12. Department of Defense Military Standard MIL-STD-1543B, *Reliability Program Requirements for Space and Launch Vehicles*, 1982

13. Department of Defense Military Standard MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis*, 1980

INITIAL DISTRIBUTION LIST

		Number of Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, California 93943-5101	2
3.	Dr. Rudolph Panholzer Chairman, Space Systems Academic Group Code SP/PZ Naval Postgraduate School Monterey, California 93943-5002	1
4.	Prof. Barry Leonard Aeronautic and Astronautics Department Code AA/LN Naval Postgraduate School Monterey, California 93943-5002	4
5.	Dr. Walter M. Woods Operations Research Department, Code OR/WO Naval Postgraduate School Monterey, California 93943-5002	1
6.	Chief of Naval Operations Navy Space Systems Command Code N63 2000 Navy Pentagon Washington, DC 20350-2000	2
7.	Lieutenant David W. Alldridge 190 Heather Drive Stanfield, Oregon 97875	2